Solutions

to

A First Course in Abstract Algebra

John B. Fraleigh
sixth edition
ISBN 0-201-33596-4
Addison Wesley Longman

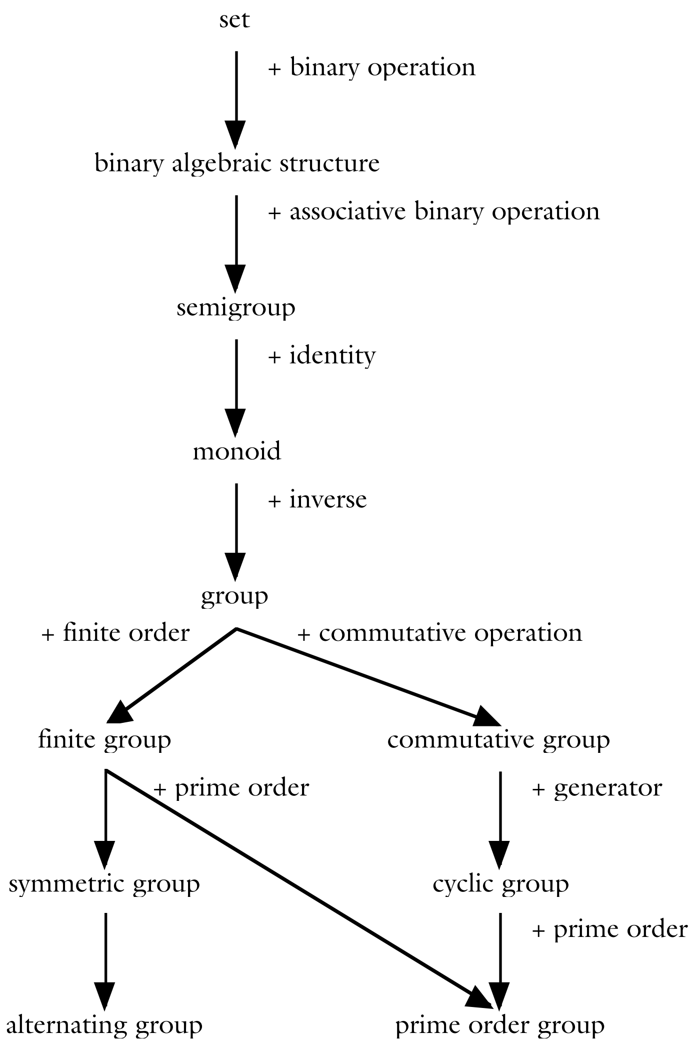
by

Ben Hekster
PO Box 391852
Mountain View, CA 94039-1852
heksterb@acm.org

http://www.hekster.org/Academic/Mathematics/

These are completely unofficial and unverified worked solutions by me. Corrections welcome.
Typeset in Galliard and Gill Sans using AppleWorks 5 on Apple Macintosh.

Abstract Algebras



Glossary

:	reads as “so that”
$+_i$, $\cdot_i$	summation, multiplication over i
$(_i \quad \{_i$	ordered, unordered set over i
$\wedge, \vee, <, >$	scalar operators
$\cap, \cup, \subset, \supset$	set operators
$=_n$	congruent modulo n
$\triangleleft$	is normal to, is ideal to
fx	function application $f\left(x\right)$
commutative group	abelian group
maximal p-group	Sylow p-group

§0.1 Preliminaries

1. proving theorems
2. set
3. precision?
4. definition
5. A triangle with vertices P, Q, R is the collection of points X such that
   - X is in the line segment PQ, or
   - X is in the line segment QR, or
   - X is in the line segment RP.
6. An **equilateral triangle** is a triangle with vertices P, Q, R such that the length of the line segment PQ equals both the length of the line segment QR and the length of the line segment RP.
7. A **right triangle** is a triangle with vertices P, Q, R in which the two line segments through one of its vertices (say PQ and PR) are such, that for any point X on PQ there is no point Y on PR such that the length of the line segment XY is less than the length of the line segment XP.
8. The **interior** of a triangle is the collection of points X such that the line segments XP, XQ, XR from X to its vertices P, Q, R have only the vertices in common with the triangle.
9. A **circle** with **center** C and **radius** r is the collection of points X such that the length of the line segment XC equals r.
10. A **disk** with **center** C and **radius** r is the collection of points X such that the length of the line segment XC is less than or equal to r.
11. Define the relationship between PQ and PR in 7. to be a **right angle**. Then, a **rectangle** with vertices P, Q, R, S is the collection of points formed by the four line segments PQ, QR, RS, SP, where PQ is at a right angle to QR, QR to RS, RS to SP, and SP to PQ.
12. Let n and m be even integers. Then by (2), there are integers p, q such that $n = 2p$, $m = 2q$. Then $n + m = 2p + 2q = 2(p + q)$, so $n + m$ is even.
13. Let n, m, p, q as in 12. Then $nm = 2p \cdot 2q = 4pq$. Since pq is an integer, $4pq$ is an integral multiple of 4.
14. Define an **odd** integer m to be an integer such that there exists another integer n such that $m = 2n + 1$.

    Let r be an even integer and s an odd integer. Then there are integers p, q such that $r = 2p$, $s = 2q + 1$. So $r + s = 2p + 2q + 1 = 2(p + q) + 1$, so $r + s$ is odd.
15. counterexample
16. A B F G M, C D J, E H K N, I, L, O.
17. 1, 2, 4, 8, 16, 31 (the conjecture is false).
18. Suppose that i is the square of an odd integer k. Then

    $$\exists i \in \mathbb{Z} : k = 2l + 1 \Rightarrow i = k^2 = (2l+1)^2 = 4l^2 + 4l + 1$$

    Since i is also even,

    $$\exists j \in \mathbb{Z} : \quad i = 2j \Rightarrow \quad 4l^2 + 4l + 1 = 2j \quad \Rightarrow \quad 2l^2 + 2l + \tfrac{1}{2} = j \notin \mathbb{Z}$$

    which is a contradiction, so k cannot be odd. Since k must be even,

    $$\exists l \in \mathbb{N} : \quad k = 2l \Rightarrow \quad i = k^2 = (2l)^2 = 4l^2$$

    so i is indeed an integral multiple of 4.
19. Let $n = 0$, then $(n+3)^2 = 3^2 = 9 \ngtr 9$.
20. Let $n^2 + 2 = 3 \Rightarrow \quad n^2 = 1 \Rightarrow \quad n = -1 \vee n = +1$, so n is not unique.
21. Let $n = 2 \Rightarrow \quad n^2 + 4 = 2^2 + 4 = 8$.
22. Let $n = 3 \Rightarrow \quad n^2 + 5 = 3^2 + 5 = 14$.
23. Let $n = -3 \Rightarrow \quad n^2 + 5 = (-3)^2 + 5 = 14$. With 22., n is not unique.
24. Let $n = 0$: $\quad n^2 > n \Leftarrow \quad 0^2 > 0$, which is a contradiction.
25. Let $n \in \mathbb{N}, n < 0 \Rightarrow \quad n^2 > 0 \Rightarrow \quad n^2 > 0 > n$.
26. Let $x = \frac{1}{2} \Rightarrow \quad x^2 < x \Leftarrow \quad \left(\frac{1}{2}\right)^2 < \frac{1}{2} \Leftarrow \quad \frac{1}{4} < \frac{1}{2}$, which is a contradiction.

27. Let $n=2$: $\quad n^2 > n \Leftarrow \quad 2^2 > 2 \Leftarrow \quad 4 > 2$.

28. Let $\begin{cases} n=0: & n^2 = n \Leftarrow \quad 0^2 = 0 \Leftarrow \quad 0=0 \\ n=1: & n^2 = n \Leftarrow \quad 1^2 = 1 \Leftarrow \quad 1=1 \end{cases}$, so x is not unique.

29. Let j be an odd integer, so

$$\begin{aligned} \exists k \in \mathbb{Z}: \quad j &= 2k+1 \\ \Rightarrow j^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= k^2 + k \in \mathbb{N} \end{aligned}$$

30. $\exists m \in \mathbb{N}: \quad n = 3m+1$, so $n^2 = (3m+1)^2 = 9m^2 + 6m + 1 = 3\left(3m^2 + 2m\right) + 1$, and $3m^2 + 2m$ is integral.

31. Let $n=-2$: $\quad n^3 < n \Leftarrow \quad (-2)^3 < -2 \Leftarrow \quad -8 < -2$.

32. Let $n=-2, m=1$: $\quad \left(\frac{n}{m}\right)^2 = \left(\frac{-2}{1}\right)^2 = (-2)^2 = 4 \nless 1$.

33. $\left(\frac{n}{m}\right)^2 < \frac{n}{m} \Rightarrow (m=0) \qquad n^2 < nm \Rightarrow (n<0) \qquad n \ge m \Rightarrow \qquad n \nless m$.

34. $\left(\frac{n}{m}\right)^3 \le \left(\frac{n}{m}\right)^2 \Rightarrow \begin{cases} m \ge 0: & n^3 \le mn^2 \Rightarrow (n \ne 0) \quad n \le m \Rightarrow \quad n < m \\ m \le 0: & n^3 \ge mn^2 \Rightarrow (n \ne 0) \quad n \ge m \Rightarrow \quad n \nless m \end{cases}$. So let $m = -1$ and $n = -2$:

$\left(\frac{n}{m}\right)^3 \le \left(\frac{n}{m}\right)^2 \Rightarrow \quad \left(\frac{-2}{-1}\right)^3 \le \left(\frac{-2}{-1}\right)^2 \Rightarrow \quad 8 \le 4$, which is a contradiction.

§0.2 Sets and Relations

♥ 17. An equivalence relation ~ extracts a property from the whole identity of its arguments and asserts the equality of just this property: equivalence is property equality. For example, 'congruence modulo' ≡ asserts equality of the remainder under division.

1. $\{x \in \mathbb{R} \mid x^2 = 3\} = \{-\sqrt{3}, +\sqrt{3}\}$

2. $\{m \in \mathbb{Z} \mid m^2 = 3\} = \varnothing$

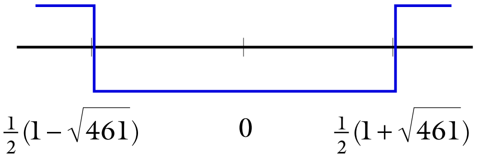
3. $\{m \in \mathbb{Z} \mid mn = 60 \text{ for some } n \in \mathbb{Z}\} = \pm\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}$

4. $\{m \in \mathbb{Z} \mid m^2 - m < 115\}$. Solve the inequality:

$$m^2 - m = 115 \Rightarrow \quad m^2 - m - 115 = 0 \Rightarrow$$

$$m = \frac{+1 \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot -115}}{2 \cdot 1} = \frac{1 \pm \sqrt{1+460}}{2}$$

$$= \tfrac{1}{2}(1 \pm \sqrt{461}) \approx -10.2, 11.2$$



so $m \in \{-10, -9, \ldots, 10, 11\}$.

5. not a set

6. $\varnothing$

7. $\varnothing$

8. $\mathbb{Q}$

9. $\mathbb{Q}$

10. $\left\{\frac{m}{2} \mid m \in \mathbb{Z}\right\}$

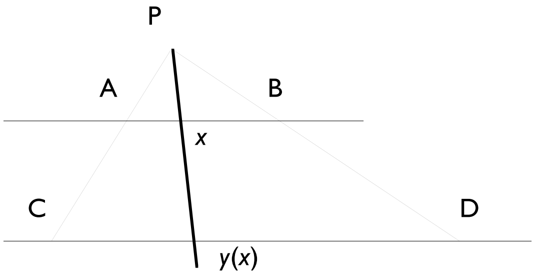
11. $\{(a,1), (a,2), (a,c), (b,1), (b,2), (b,c), (c,1), (c,2), (c,c)\}$

12.

	function	one-to-one	onto
a.	yes	no	no
b.	yes	no	no
c.	no		

d.	yes	yes	yes
e.	yes	no	no
f.	no		

13. Map x to $y(x)$.



14 a. $f:[0,1]\to[0,2]: x\mapsto 2x$

b. $f:[1,3]\to[5,25]: x\mapsto (x-1)\,\frac{20}{2}+5$

c. $f:[a,b]\to[c,d]: x\mapsto (x-a)\,\dfrac{d-c}{b-a}+c$

15. $f: S\to\mathbb{R}: x\mapsto \tan\left(x\pi-\tfrac{1}{2}\pi\right)$

16. a. $\mathcal{P}(\varnothing)=\varnothing,\quad \left|\mathcal{P}(\varnothing)=1\right|$

b. $\mathcal{P}(\{a\})=\left\{\varnothing,\{a\}\right\},\quad \left|\mathcal{P}(\{a\})\right|=2$

c. $\mathcal{P}(\{a,b\})=\left\{\varnothing,\{a\},\{b\},\{a,b\}\right\},\quad \left|\mathcal{P}(\{a,b\})\right|=4$

d. $\mathcal{P}(\{a,b,c\})=\left\{\varnothing,\{a\},\{b\},\{a,b\},\{c\},\{a,c\},\{b,c\},\{a,b,c\}\right\},\quad \left|\mathcal{P}(\{a,b,c\})\right|=8$

17. Conjecture $\left|\mathcal{P}(A)\right|=2^{|A|}$.

Let A_n be a series of sets such that $|A_n| = n$, and $A_n\subset A_{n+1}$.

- $\left|\mathcal{P}(A_0)\right|=\left|\mathcal{P}(\varnothing)\right|=1$.
- Let $\left|\mathcal{P}(A_n)\right|=2^{|A_n|}$.

There is $s_{n+1}\notin A_n$ such that $A_{n+1}=A_n\cup s_{n+1}$. Consider the set

$$A'_n=\bigcup\nolimits_{P\subseteq A_n} P\cup\left(P\cup\{s_{n+1}\}\right)$$

Since every element of A'_n is a subset of A_{n+1}, $A'_n\subseteq\mathcal{P}(A_{n+1})$.

Every subset P of A_{n+1} either does or does not contain s_{n+1}:

$s_{n+1}\notin P\Rightarrow\quad P\subseteq A_n\Rightarrow\quad P\in A'_n$
$s_{n+1}\in P\Rightarrow\quad P\setminus\{s_{n+1}\}\subseteq A_n\Rightarrow\quad P\in A'_n$
so $\mathcal{P}(A_{n+1})\subseteq A'_n$.

So $\mathcal{P}(A_{n+1})=A'_n$, and $\left|\mathcal{P}(A_{n+1})\right|=2\cdot\left|\mathcal{P}(A_n)\right|=2\cdot 2^{|A_n|}=2^{|A_n|+1}=2^{|A_{n+1}|}$.

18. Let $\left(f:A\to B\right)\in B^A$.

- For each subset $P\subseteq A$, there is a corresponding function

$$f_P: A\to B: a\mapsto\begin{cases}a\notin P: 0\\ a\in P: 1\end{cases}$$

Let there be two such subsets $P, P'\subseteq A$ such that $f_P=f_{P'}$. Then $\forall a\in A$:

$a\in P\Rightarrow\quad f_P(a)=f_{P'}(a)=1\Rightarrow\quad a\in P'$; $a\notin P\Rightarrow\ldots\Rightarrow a\notin P'$
so $P=P'$.

- Conversely, for each function $f \in B^A$ there is a corresponding subset $P_f \subseteq A$:

  $P_f = \{a \in A \mid f(a) = 1\}$.

  Let there be two functions $f, f' \in B^A$ such that $P_f = P_{f'}$. Then $\forall a \in A$:

  $$\vee\begin{cases} f(a) = 0 \\ f(a) = 1 \end{cases} \Rightarrow \quad \vee\begin{cases} a \notin P_f \\ a \in P_f \end{cases} \Rightarrow \quad \vee\begin{cases} f'(a) = 0 \\ f'(a) = 1 \end{cases}$$

  so $f = f'$.

  So, $P_f\colon B^A \to \mathcal{P}(A)$ is a bijection, and $\left|B^A\right| = \left|\mathcal{P}(A)\right|$.

19. For every element of A there is a distinct singleton subset containing just that element, which is an element of $\mathcal{P}(A)$. $\varnothing$ is not such a singleton set, yet is an element of $\mathcal{P}(A)$. So $\left|\mathcal{P}(A)\right| > |A|$.

    Let A be such that $|A| = \aleph$. Then the power set of A has $\left|\mathcal{P}(A)\right| > \aleph$, and $\left|\mathcal{P}\big(\mathcal{P}(A)\big)\right| > \left|\mathcal{P}(A)\right|$, ad infinitum.

20. a. It is possible to define addition in $\mathbb{N}$ in terms of the union of disjoint sets, so

    $2 + 3 = 5 \Leftarrow \quad |A| = 2, |B| = 3, |A \cup B| = 5$.

    i. $3 + \aleph_0 = \left|\{0\} \cup \mathbb{Z}^+\right| \overset{(*)}{=} \left|\mathbb{Z}^+\right| = \aleph_0$, where $(*)$: $\quad \phi : \mathbb{Z}^+ \to \{0\} \cup \mathbb{Z}^+ : m \mapsto m - 1$.

    ii. $\aleph_0 + \aleph_0 = \left|\left(\mathbb{Z}^+ - \tfrac{1}{2}\right) \cup \mathbb{Z}^+\right| \overset{(*)}{=} \left|\mathbb{Z}^+\right| = \aleph_0$, where $(*)$ $\quad \phi : \mathbb{Z}^+ \to \left(\mathbb{Z}^+ - \tfrac{1}{2}\right) \cup \mathbb{Z}^+ : m \mapsto \begin{cases} m \text{ odd}: & \tfrac{1}{2}(m-1) + \tfrac{1}{2} \\ m \text{ even}: & \tfrac{1}{2}m \end{cases}$.

    b. It is possible to define multiplication in $\mathbb{N}$ in terms of a Cartesian product:

    $2 \cdot 3 = \left|\{1, 2\} \times \{1, 2, 3\}\right| = 6$, so

    $\aleph_0 \cdot \aleph_0 = \left|\mathbb{Z}^+ \times \mathbb{Z}^+\right| \overset{\text{fig 14}}{=} \left|\mathbb{Z}^+\right| = \aleph_0$.

21. 10^2 digits, 10^5 digits. By extrapolation, $10^{\aleph_0}$ would equal the number of digits of the form 0.###..., where '#' is repeated $\aleph_0$ times— name this set R. Since any number in $R' = \{x \in \mathbb{R} \mid 0 \le x < 1\}$ can be expressed arbitrarily precise by an element of R, $R' \subseteq R$. Since $R \subseteq R'$, $R = R'$. By Exercise 15, $|R'| = \aleph$, so $|R| = \aleph$ and $10^{\aleph_0} = \aleph$.

    Similar arguments can be made in terms of duodecimal and binary expansions of numbers of R', so $12^{\aleph_0} = 2^{\aleph_0} = \aleph$.

22. Since

    $$\left|\mathcal{P}(\mathbb{Z})\right| \overset{(17)}{=} 2^{|\mathbb{Z}|} = 2^{\aleph_0} \overset{(18)}{=} \aleph; \quad \left|\mathcal{P}(\mathbb{Z})\right| \overset{(19)}{=} \left|\{0,1\}^{\mathbb{Z}}\right|$$

    The next higher cardinals after $\aleph_0$ are

    $\aleph = \left|\{0,1\}^{\mathbb{Z}}\right| = \{0,1\} \exp \mathbb{Z}$,

    $\left|\{0,1\}^{\{0,\, 1\}^{\mathbb{Z}}}\right| = \{0,1\} \exp \{0,1\} \exp \mathbb{Z}$

    et cetera.

28. $x \mathrel{\mathrm{R}} y \Rightarrow \exists i\colon x, y \in P_i \Rightarrow y, x \in P_i \Rightarrow y \mathrel{\mathrm{R}} x$ (symmetric)

    $x \mathrel{\mathrm{R}} x \Leftrightarrow \exists i\colon x \in P_i \Leftrightarrow x \in S$ (reflexive)

    $x \mathrel{\mathrm{R}} y \wedge y \mathrel{\mathrm{R}} z \Rightarrow \exists i\colon x, y \in P_i \wedge \exists j\colon y, z \in P_j$

    $\qquad \Rightarrow (P_i \text{ disjoint} \Rightarrow i = j)\ \exists i\colon x, y, z \in P_i$ (transitive).

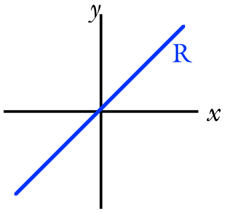
    $\qquad \Rightarrow y \mathrel{\mathrm{R}} z$

29. not reflexive because $0 \cdot 0 \not> 0 \Rightarrow 0 \not\mathrel{\mathrm{R}} 0$

30. not symmetric because $2 \ge 1, 1 \not\ge 2 \Rightarrow 2 \mathrel{\mathrm{R}} 1, 1 \not\mathrel{\mathrm{R}} 2$.

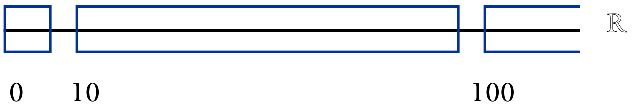
31. R is a relation, because

$$\begin{cases} |x| = |x| \\ |x| = |y| \Rightarrow |y| = |x| \\ |x| = |y| \wedge |y| = |x| \Rightarrow |x| = |z| \end{cases} \Rightarrow \begin{cases} x \mathrel{R} x \\ x \mathrel{R} y \Rightarrow y \mathrel{R} x \\ x \mathrel{R} y \wedge y \mathrel{R} z \Rightarrow x \mathrel{R} z \end{cases} .$$



32. $|0-3| = 3 \leq 3, \quad |3-6| = 3 \leq 3, \quad |0-6| = 6 \not\leq 3 \Rightarrow$ so R is not transitive.
$0 \mathrel{R} 3, \quad 3 \mathrel{R} 6, \quad 0 \not\mathrel{R} 6$

33. The number of digits of $n \in \mathbb{Z}^+$ is base 10 notation is $1 + \left\lfloor {}^{10}\log n \right\rfloor$. Obviously R is reflexive and symmetric, and transitive.



34. R is congruence modulo 10 on $\mathbb{Z}^*$.

35. a. {1, 3, 5, …}, {2, 4, 6, …}
b. {1, 4, 7, …}, {2, 5, 8, …}, {3, 6, 9, …}
c. {1, 6, 11, …}, {2, 7, 12, …}, {3, 8, 13, …}, {4, 9, 14, …}, {5, 10, 15, …}

36a.

$$\forall r \in \mathbb{Z}: \quad r - r = 0 = 0 \cdot n \Rightarrow r \sim r$$

$$\forall r,s, r \sim s: \quad \exists q \in \mathbb{Z}: \quad r - s = qn \Rightarrow s - r = -(qn) = (-q)n \Rightarrow s \sim r$$

$$\forall r,s,t, r \sim s, s \sim t: \quad \exists p,q \in \mathbb{Z}: \qquad r - s = pn,\ s - t = qn$$

$$r - s + s - t = pn + qn$$

$$r - t = (p+q)n \Rightarrow r \sim t$$

b. $\forall r,s \in \mathbb{Z}^+, r \sim s: \quad \exists q \in \mathbb{Z}: \quad r - s = qn \Rightarrow (n \in \mathbb{Z}) \dfrac{r-s}{n} = \dfrac{r}{n} - \dfrac{s}{n} = q$

$\exists r'_n, s'_n \in \mathbb{Z}, r''_n, s''_n \in \mathbb{N}: \quad r = r'_n n + r''_n,\ s = s'_n n + s''_n,\ 0 \leq r''_n, s''_n < n$

$$r - s = qn$$

$$r'_n n + r''_n - s'_n n - s''_n = qn$$

$$(r'_n - s'_n)n + (r''_n - s''_n) = qn$$

$$r'_n - s'_n + \frac{(r''_n - s''_n)}{n} = q \quad \wedge \quad 0 \leq \frac{r''_n - s''_n}{n} < 1$$

Since $r'_n, s'_n \in \mathbb{N}, q \in \mathbb{Z}, \dfrac{r''_n - s''_n}{n} = 0 \quad \Rightarrow r''_n - s''_n$.

c.

{…, –2, 1, 3, …}, {…, –2, 0, 2, …}
{…, –2, 1, 4, …}, {…, –1, 2, 5, …}, {…, –3, 0, 3, …}
{…, –4, 1, 6, …}, {…, –3, 2, 7, …}, {…, –2, 3, 8, …}, {…, –1, 4, 9, …}, {…, –5, 0, 5, …}

§0.3 Mathematical Induction

1. Prove that $\underset{i=1\ldots n}{+} i^2 = \dfrac{n(n+1)(2n+1)}{6}$.

$$n = 1: \quad 1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6} = \frac{2 \cdot 3}{6} = 1$$

$$n+1: \quad \underset{i\ldots n+1}{+} i^2 = \underset{i\ldots n}{+} i^2 + \left(n+1\right)^2 = \frac{n\left(n+1\right)\left(2n+1\right)}{6} + n^2 + 2n + 1 = \frac{n\left(n+1\right)\left(2n+1\right) + 6\left(n^2+2n+1\right)}{6}$$

$$= n\left(2n^2+3n+1\right) + 6n^2 + 12n + 6 = \ldots = \left(n+1\right)\left(n+2\right)\left(2n+3\right)$$

2. Prove that $\underset{i=1\ldots n}{+} i^3 = \dfrac{n^2\left(n+1\right)^2}{4}, n \in \mathbb{Z}^+$.

$$n=1: \quad 1^3 = \frac{1^2\left(1+1\right)^2}{4} = \frac{1\cdot 2^2}{4} = 1$$

$$n+1: \quad \underset{1\ldots n+1}{+} i^3 = \underset{i\ldots n}{+} i^3 + \left(n+1\right)^3 = \frac{n^2\left(n+1\right)^2}{4} + \left(n+1\right)\left(n+1\right)^2$$

$$= \frac{n^2\left(n^2+2n+1\right) + 4\left(n+1\right)\left(n^2+2n+1\right)}{4} = \frac{n^4+2n^3+n^2+4n^3+8n^2+4n+4n^2+8n+4}{4}$$

$$= \frac{n^4+6n^3+13n^2+12n+4}{4} = \ldots = \frac{\left(n+1\right)^2\left(n+2\right)^2}{4}$$

3. Prove that $\underset{i=1\ldots n}{+}\left(2i-1\right) = n^2$.

$$n=1: \quad 1 = 1^2$$

$$n+1: \quad \underset{i=1\ldots n+1}{+}\left(2i-1\right) = \underset{i=i\ldots n}{+}\left(2i-1\right) + 2\left(n+1\right) - 1 = n^2 + 2n + 1 = \left(n+1\right)^2$$

4. Prove that $\underset{i=1\ldots n}{+}\dfrac{1}{i\left(i+1\right)} = \dfrac{n}{n+1}, n \in \mathbb{Z}^+$.

$$n=1: \quad \frac{1}{1\left(1+1\right)} = \tfrac{1}{2} = \frac{1}{1+1} = \tfrac{1}{2}$$

$$n+1: \quad \underset{i=1\ldots n+1}{+}\frac{1}{i\left(i+1\right)} = \underset{i=1\ldots n}{+}\frac{1}{i\left(i+1\right)} + \frac{1}{\left(n+1\right)\left(n+2\right)} = \frac{n}{n+1} + \frac{1}{\left(n+1\right)\left(n+2\right)}$$

$$= \frac{n\left(n+2\right)+1}{\left(n+1\right)\left(n+2\right)} = \frac{n^2+2n+1}{\left(n+1\right)\left(n+2\right)} = \frac{\left(n+1\right)^2}{\left(n+1\right)\left(n+2\right)} = \frac{n+1}{n+2}$$

5. Prove that $\forall a, r \in \mathbb{R}, r \neq 1, n \in \mathbb{R}^+ : \quad \overset{n}{\underset{i=0}{+}} ar^i = \dfrac{a\left(1-r^{n+1}\right)}{1-r}$.

$$n=1: \quad a + ar = \frac{a\left(1-r^2\right)}{1-r} = \frac{a\left(1-r\right)\left(1+r\right)}{1-r} = a\left(1-r\right)$$

$$n+1: \quad \overset{n+1}{\underset{i=0}{+}} ar^i = \overset{n}{\underset{i=0}{+}} ar^i + ar^{n+1} = \frac{a\left(1-r^{n+1}\right)}{1-r} + ar^{n+1} = \frac{a\left(1-r^{n+1}\right) + \left(1-r\right)ar^{n+1}}{1-r}$$

$$= a\frac{1-r^{n+1}+\left(1-r\right)r^{n+1}}{1-r} = a\frac{1-r^{n+1}+r^{n+1}-r^{n+2}}{1-r} = \frac{a\left(1-r^{n+2}\right)}{1-r}$$

6. max is only defined on $\mathbb{Z}^+$, so $\max(i-1, j-1)$ is undefined.

7. the concept ‘interesting property’ is not well defined

§0.4 Complex and Matrix Algebra

1. $\left(2+3i\right)+\left(4+5i\right) = 6+2i$.

2. $i+5-3i = 5-2i$.

3. $(5+7i)-(3-2i)=2+5i$.

4. $(1-3i)-(-4+2i)=5-5i$.

5. $i^3 = ii^2 = -i$.

6. $i^4 = i^2 \cdot i^2 = -1 \cdot -1 = +1$.

7. $i^{23} = i^{20} i^3 = (i^4)^5 \cdot i^3 = 1^5 \cdot i^3 = -i$.

8. $(-i)^{35} = -i^{35} = -(i^{32} i^3) = -(1 \cdot -i) = i$.

9. $(4-i)(5+3i) = 20 + 12i - 5i - 3i^2 = 23 + 7i$.

10. $(8+2i)(3-i) = 24 + 6i - 8i - 2i^2 = 26 - 2i$.

11. $(2-3i)(4+i)+(6-5i) = 8 + 2i - 12i - 3i^2 + 6 - 5i = 17 - 15i$.

12. $(1+i)^3 = (1+i)(1+i)^2 = (1+i)(1+2i+i^2) = (1+i)2i = 2i + 2i^2 = -2 + 2i$.

14. $\dfrac{7-5i}{1+6i} = \dfrac{(7-5i)(1-6i)}{(1+6i)(1-6i)} = \dfrac{7-42i-5i+30i^2}{1-36} = \tfrac{1}{35}(-23-47i)$.

15. $\dfrac{1}{1+i} = \dfrac{i(1-i)}{(1+i)(1-i)} = \dfrac{i-i^2}{1-i^2} = \dfrac{i+1}{2}$.

16. $\dfrac{1-i}{i} = \dfrac{(1-i)i}{i^2} = -(i-i^2) = -1-i$.

17. $\dfrac{i(3+i)}{2-4i} = \dfrac{1}{2} \cdot \dfrac{i(3+i)(1+2i)}{(1-2i)(1+2i)} = \tfrac{1}{2}\dfrac{(3i-1)(1+2i)}{1^2-4i^2} = \tfrac{1}{10}(-1+3i-2i+6i^2) = \tfrac{1}{10}(-7+i)$.

18.
$$\frac{3+7i}{(1+i)(2-3i)} = \frac{(3+7i)(1-i)(2+3i)}{(1+i)(1-i)(2-3i)(2+3i)} = \frac{(3-3i+7i-7i^2)(2+3i)}{(1-i^2)(4-9i^2)}$$
$$= \frac{(10+4i)(2+3i)}{2 \cdot 13} = \frac{(5+2i)(2+3i)}{13} = \frac{10+15i+4i+6i^2}{13} = \frac{4+19i}{13}.$$

19. $\dfrac{(1-i)(2+i)}{(1-2i)(1+i)} = \dfrac{(1-i)^2(2+i)(1+2i)}{(1-2i)(1+2i)(1+i)(1-i)} = \dfrac{(1-2i+i^2)(2+4i+i+2i^2)}{(1-4i^2)(1-i^2)} = \dfrac{-2i \cdot 5i}{5 \cdot 2} = \dfrac{-i^2}{1} = 1$.

20. $|3-4i| = 5$.

21. $|6+4i| = 2|3+2i| = 2\sqrt{9+4} = 2\sqrt{13}$.

22. $|3-4i| = 5 \quad \Rightarrow 3-4i = 5\left(\tfrac{3}{5} - \tfrac{4}{5}i\right)$.

23. $|-1+i| = \sqrt{2} \quad \Rightarrow -1+i = \sqrt{2}\left(-\dfrac{1}{\sqrt{2}} + i\dfrac{1}{\sqrt{2}}\right) = \sqrt{2}\left(-\tfrac{1}{2}\sqrt{2} + \tfrac{1}{2}i\sqrt{2}\right)$.

24. $|12+5i| = \sqrt{144+25} = \sqrt{169} = 13 \quad \Rightarrow 12+5i = 13\left(\tfrac{12}{13} + \tfrac{5}{13}i\right)$.

25. $|-3+5i| = \sqrt{9+25} = \sqrt{36} = 6 \quad \Rightarrow -3+5i = 6\left(-\tfrac{1}{2} + \tfrac{5}{6}i\right)$.

26. $z_1 = r_1 e^{i\theta_1}, z_2 = r_2 e^{i\theta_2} \Rightarrow \quad z_1/z_2 = z_1 z_2^{-1} = r_1 e^{i\theta_1} \cdot \left(r_2 e^{i\theta_2}\right)^{-1} = \dfrac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$. So z_1/z_2 is the point in the complex point at the end of a line from the origin with length r_1/r_2 and angle $\theta_1 - \theta_2$ from the positive *x*-axis.

27. $z^4 = 1 \quad \Rightarrow \left(re^{i\theta}\right)^4 = 1e^{0i} \quad \Rightarrow r = 1, 4\theta =_{2\pi} 0 \quad \Rightarrow r = 1, \theta =_{\frac{1}{2}\pi} 0 \quad \Rightarrow z \in \left\{1, i, -1, -i\right\}.$

28. $z^4 = -1 \quad \Rightarrow \left(re^{i\theta}\right)^4 = 1e^{i\pi} \quad \Rightarrow r = \sqrt[4]{1}, 4\theta =_{2\pi} i\pi \quad \Rightarrow r = 1, \theta =_{\frac{1}{2}\pi} \frac{1}{4}\pi$.

$$\Rightarrow z \in \left\{\tfrac{1}{2}\sqrt{2} + \tfrac{1}{2}i\sqrt{2}, -\tfrac{1}{2}\sqrt{2} + i\tfrac{1}{2}\sqrt{2}, -\tfrac{1}{2}\sqrt{2} - \tfrac{1}{2}i\sqrt{2}, \tfrac{1}{2}\sqrt{2} - \tfrac{1}{2}i\sqrt{2}\right\}$$

§1.1 Binary Operations

1. $b * d = e, c * c = b, \left(\left(a * c\right) * e\right) * a = \left(c * e\right) * a = a * a = a.$

2. $\begin{array}{l} \left(a * b\right) * c = b * c = a \\ a * \left(b * c\right) = a * a = a \end{array}$, so * could be, but is not necessarily, associative.

3. $\begin{array}{l} \left(b * d\right) * c = e * c = a \\ b * \left(d * c\right) = b * b = c \end{array}$, so * is not associative.

4. no, because $e * b \neq b * e$.

5.

*	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

6.

*	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d	d	c	c	d

$d * a = \left(c * b\right) * a = c * \left(b * a\right) = c * b = d,$

$d * b = \left(c * b\right) * b = c * \left(b * b\right) = c * a = c,$

$d * c = \left(c * b\right) * c = c * \left(b * c\right) = c * c = c,$

$d * d = \left(c * b\right) * d = c * \left(b * d\right) = c * d = d.$

7. $1 * 0 = 1 - 0 = 1, \quad 0 * 1 = 0 - 1 = -1, \ \left(a * b\right) * c = \left(a - b\right) - c = a - b - c, \ a * \left(b * c\right) = a - \left(b - c\right) = a - b + c$, so * is neither commutative nor associative.

8. Let $\forall a,b \in \mathbb{Q}: \quad a * b = ab + 1 = ba + 1 = b * a, \ \left(0 * 0\right) * 1 = \left(0 \cdot 0 + 1\right) \cdot 1 + 1 = 2, \ 0 * \left(0 * 1\right) = 0 \cdot \left(0 \cdot 1 + 1\right) + 1 = 1$, so * is commutative, but not associative.

9. $\forall a,b \in \mathbb{Q}: \quad a * b = \frac{1}{2}ab = \frac{1}{2}ba = b * a, \ \forall a,b,c \in \mathbb{Q}: \quad \left(a * b\right) * c = \frac{1}{2}\left(\frac{1}{2}ab\right)c = \frac{1}{2}a\left(\frac{1}{2}bc\right) = a * \left(b * c\right)$, so * is commutative and associative.

10. Let $\forall a,b \in \mathbb{Z}^+: \quad a * b = 2^{ab} = 2^{ba} = b * a$, then $0 * \left(0 * 1\right) = 2^{0 \cdot 2^{0 \cdot 1}} = 2^0 = 1$ and $\left(0 * 0\right) * 1 = 2^{2^{0 \cdot 0} \cdot 1} = 2^1 = 2$, so * is commutative, but not associative.

11. $1 * 2 = 1^2 = 1; \quad 2 * 1 = 2^1 = 2$ and $2 * \left(3 * 2\right) = 2^{\left(3^2\right)} = 2^9; \quad \left(2 * 3\right) * 2 = \left(2^3\right)^2 = 2^6$, so * is neither commutative nor associative.

12. 1; $\quad 2^{2^2} = 2^4 = 16; \quad 3^{3^3} = 3^9 = 19683; \quad n^{n^n}$; the table defining * has n^2 entries, each having n possible values.

13. 1; $\quad 2^{\frac{1}{2} \cdot 2\left(2-1\right)} = 2^1 = 2; \quad 3^{\frac{1}{2} \cdot 3\left(3-1\right)} = 3^3 = 27; \quad n^{\frac{1}{2}n\left(n-1\right)}$; the table defining commutative * has $\frac{1}{2}n\left(n-1\right)$ entries, each having n possible values.

14. A binary operation on a set *S* is commutative if and only if for all $a, b \in S$: $a * b = b * a$.

15. well defined

16. Correct the last part to read "$a, b \in H$".

17. C1 good; $1 * 2 = 1 - 2 = -1 \in Z^+$, so C2 is ill defined.

18. C1, C2 good.

19. C1, C2 good.

20. C1, C2 good.

21. C1 is not well defined, C2 is good.

22. C1 good; $1 * 1 = 0 \notin \mathbb{Z}^+$, so C2 is ill defined.

23. $\forall M = \begin{bmatrix} a & -b \\ -b & a \end{bmatrix}, N = \begin{bmatrix} c & -d \\ -d & c \end{bmatrix} \notin H:$

a. $\begin{bmatrix} a & -b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & -b-d \\ -b-d & a+c \end{bmatrix} \in H$

b. $\begin{bmatrix} a & -b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ -d & c \end{bmatrix} = \begin{bmatrix} a \cdot c - b \cdot -d & a \cdot -d - b \cdot c \\ -b \cdot c + a \cdot -d & -b \cdot -d + a \cdot c \end{bmatrix} = \begin{bmatrix} ac + bd & -ad - bc \\ -ad - bc & ac + bd \end{bmatrix} \in H$

24. a. false; b. true; c. false; d. false; e. false; f. true; g. true; h. true; i. true; j. false.

25. Let * be addition and *' subtraction on the set of colors {K, R, G, B, C, M, Y, W} (black, red, green, blue, cyan, magenta, yellow, and white).

+	*K*	*R*	*G*	*B*	*C*	*M*	*Y*	*W*
K	*K*							
R	*R*	*R*						
G	*G*	*Y*	*G*					
B	*B*	*M*	*C*	*B*				
C	*C*	*W*	*C*	*C*	*C*			
M	*M*	*M*	*W*	*M*	*W*	*M*		
Y	*Y*	*Y*	*Y*	*W*	*W*	*W*	*Y*	
W	*W*	*W*	*W*	*W*	*W*	*W*	*W*	*W*

-	*K*	*R*	*G*	*B*	*C*	*M*	*Y*	*W*
K	*K*	*K*	*K*	*K*	*K*	*K*	*K*	*K*
R	*R*	*K*	*R*	*R*	*R*	*K*	*K*	*K*
G	*G*	*G*	*K*	*G*	*K*	*G*	*K*	*K*
B	*B*	*G*	*B*	*K*	*K*	*K*	*B*	*K*
C	*C*	*C*	*B*	*G*	*K*	*G*	*B*	*K*
M	*M*	*B*	*M*	*R*	*R*	*K*	*B*	*K*
Y	*Y*	*Y*	*R*	*Y*	*R*	*G*	*K*	*K*
W	*W*	*W*	*W*	*W*	*W*	*W*	*W*	*W*

26. $(a * b) * (c * d) = (c * d) * (a * b) = (d * c) * (a * b) = ((d * c) * a) * b$

27. Let *S* be a set with single element *s*.
A binary operation * on S always maps its operands to *s*, so * must be associative and commutative.

28. Let * be the binary operation defined by the table. Then
$(b * a) * a = a * a = b$ and $b * (a * a) = b * b = a$, so * is not associative.

*	*a*	*b*
a	*b*	*a*
b	*a*	*a*

29. Let $f, g, h \in F$. Then $\forall x \in \mathbb{R}$:

$$\begin{aligned} ((f + g) + h)(x) &= (f + g)(x) + h(x) = f(x) + g(x) + h(x) \\ &= f(x) + (g + h)(x) = (f + (g + h))(x) \end{aligned}$$

, so + is associative on *F*.

30. Let $f : \mathbb{R} \to \mathbb{R} : x \mapsto 0$, $g : \mathbb{R} \to \mathbb{R} : x \mapsto 1$, then

$(f - g)(0) = f(0) - g(0) = 0 - 1 = -1$

$(g - f)(0) = g(0) - f(0) = 1 - 0 = 1$

so – is not commutative on *F*.

31. Let $f : \mathbb{R} \to \mathbb{R} : x \mapsto 1$, then

$$\big((f-f)-f\big)(0)=(f-f)(0)-f(0)=\big(f(0)-f(0)\big)-f(0)=(1-1)-1=-1$$
$$\big(f-(f-f)\big)(0)=f(0)-(f-f)(0)=f(0)-\big(f(0)-f(0)\big)=1-(1-1)=1$$

so – is not associative on *F*.

32. $\forall f,g\in F, x\in\mathbb{R}:\ (fg)(x)=f(x)\cdot g(x)=g(x)\cdot f(x)=(gf)(x)$, so multiplication is commutative on *F*.

33. For $\forall f,g\in F, x\in\mathbb{R}$,

$$\big((fg)h\big)(x)=(fg)(x)\cdot h(x)=\big(f(x)\cdot g(x)\big)\cdot h(x)=f(x)\cdot\big(g(x)\cdot h(x)\big)=f(x)\cdot(gh)(x)=\big(f(gh)\big)(x),$$

so multiplication is associative on *F*.

34. Let $f:\mathbb{R}\to\mathbb{R}: x\mapsto x+1,\quad g:\mathbb{R}\to\mathbb{R}: x\mapsto x^2$, then

$$(f\circ g)(1)=f\big(g(1)\big)=f(1)=2$$
$$(g\circ f)(1)=g\big(f(1)\big)=g(2)=4$$

so concatenation is not commutative on *F*.

35. Let $*=+,\quad *'=\cdot,\quad S=\mathbb{R}$. Then

$$1*(0*'3)=1+(0\cdot 3)=1+0=1$$
$$(1*0)*'(1*3)=(1+0)\cdot(1+3)=1\cdot 4=4$$

so the property does not hold.

36. For $\forall h,h'\in H$:

$$(h*h')*x\overset{*\text{ associative}}{=}h*(h'*x)\overset{h\text{ commutative}}{=}(h'*x)*h\overset{*\text{ associative}}{=}(x*h')*h\overset{*\text{ associative}}{=}h'*(h*x)$$

37. For $\forall a,b\in H$:

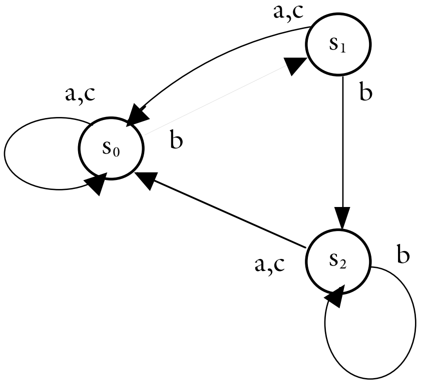
$$(a*b)*(a*b)=(a*b)*(b*a)=\big((a*b)*b\big)*a=\big(a*(b*b)\big)*a$$
$$=(a*b)*a=(b*a)*a=b*(a*a)=b*a=a*b$$

so $a*b\in H$.

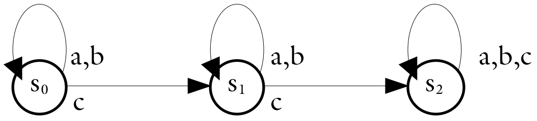
38. (deposit deposit) talk (deposit press press) = (deposit deposit deposit press) talk (press)

39. “(” doesn't affect whatever symbol is next on input.

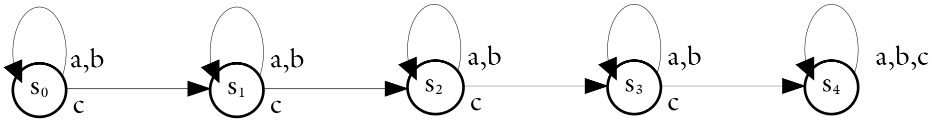
40.



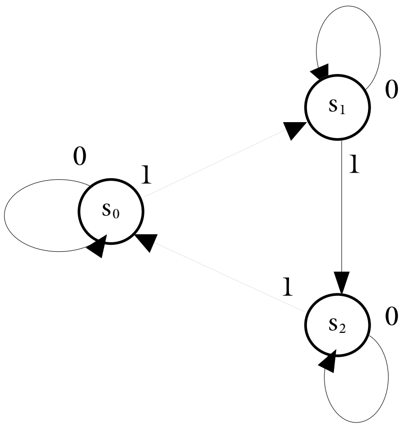
41.



42.



43.



44.

	0	1
s0	s0	s1
s1	s0	s2
s2	s0	s2

45.

	a	b	c
s0	s0	s0	s1
s1	s1	s1	s2
s2	s2	s2	s2

§1.2 Isomorphic Binary Structures

1. • ϕ is a surjection and injection (bijection)

   • $\forall s, t \in S$: $\phi\left(s * t\right) = \phi s * \phi t$.

2. $\forall m \in \mathbb{Z}: \quad \exists n \in \mathbb{Z}: \quad n = -m \Rightarrow \quad \phi n = -n = -\left(-m\right) = m$ (surjection)

   $\forall n_1, n_2 \in \mathbb{Z}: \quad \phi n_1 = \phi n_2 \Rightarrow \quad -n_1 = -n_2 \Rightarrow \quad n_1 = n_2$ (injection)

   $\forall n_1, n_2: \quad \phi\left(n_1 + n_2\right) = -\left(n_1 + n_2\right) = \left(-n_1\right) + \left(-n_2\right) = \phi n_1 + \phi n_2$

3. $1 \in$ Z, $\nexists n \in \mathbb{Z}: \quad \phi n = 2n = 1$, so ϕ is not surjective.

4. For $\forall n_1, n_2 \in \mathbb{Z}$,

   $\phi\left(n_1 + n_2\right) = \left(n_1 + n_2\right) + 1 = n_1 + n_2 + 1$

   $\phi n_1 + \phi n_2 = \left(n_1 + 1\right) + \left(n_2 + 1\right) = n_1 + n_2 + 2$

   so ϕ is not an isomorphism.

5. $\forall y \in \mathbb{Q}: \quad \exists x \in \mathbb{Q}: \quad x = 2y \Rightarrow \quad \phi x = \frac{1}{2}x = \frac{1}{2} \cdot 2y = y$ (surjection)

   $\forall x_1, x_2 \in \mathbb{Q}: \quad \phi x_1 = \phi x_2 \Rightarrow \quad \frac{1}{2}x_1 = \frac{1}{2}x_2 \Rightarrow \quad x_1 = x_2$ (injection)

   $\forall x_1, x_2 \in \mathbb{Q}: \quad \phi\left(x_1 + x_2\right) = \frac{1}{2}\left(x_1 + x_2\right) = \frac{1}{2}x_1 + \frac{1}{2}x_2 = \phi x_1 + \phi x_2$.

6. $-1 \in \mathbb{Q}, \nexists x \in \mathbb{Q}: \quad x^2 = -1$, so ϕ is not surjective.

7. $\forall y \in \mathbb{R}: \quad \exists x \in \mathbb{R}: \quad x = \sqrt[3]{y} \Rightarrow \quad \phi x = x^3 = \left(\sqrt[3]{y}\right)^3 = y$

   $\forall x_1, x_2 \in \mathbb{R}: \quad \phi x_1 = \phi x_2 \Rightarrow \quad x_1^3 = x_2^3 \Rightarrow \quad x_1 = x_2$

   $\forall x_1, x_2 \in \mathbb{R}: \quad \phi\left(x_1 \cdot x_2\right) = \left(x_1 x_2\right)^3 = x_1^3 \cdot x_2^3 = \phi x_1 \cdot \phi x_2$

8. $\begin{vmatrix} 0 & 0 \\ 0 & 0 \end{vmatrix} = 0, \quad \begin{vmatrix} 0 & 0 \\ 1 & 0 \end{vmatrix} = 0$, so ϕ is not injective.

9. $\forall y \in \mathbb{R}: \quad \exists X \in M_1\mathbb{R}: \quad X = \left[y\right]$ (surjective)

$\forall X_1, X_2 \in M_1\mathbb{R}: \quad \phi X_1 = \phi X_2 \Rightarrow \quad |X_1| = |X_2| \Rightarrow \quad x_1 = x_2 \Rightarrow \quad [x_1] = [x_2] \Rightarrow \quad X_1 = X_2$ (injective)

$\forall X_1, X_2 \in M_1\mathbb{R}: \quad \phi(X_1 \cdot X_2) = |X_1 X_2| = |[x_1] \cdot [x_2]| = |[x_1 x_2]| = x_1 x_2 = |x_1| \cdot |x_2| = \phi X_1 \cdot \phi X_2.$

10. $\forall y \in \mathbb{R}^+: \quad \exists x \in \mathbb{R}: \quad x = -{}^2\ln y \Rightarrow \quad \phi x = 0.5^x = 0.5^{-{}^2\ln y} = 2^{{}^2\ln y} = y$ (surjective)

$\forall x_1, x_2 \in \mathbb{R}: \quad \phi x_1 = \phi x_2 \Rightarrow \quad 0.5^{x_1} = 0.5^{x_2} \Rightarrow \quad x_1 = x_2$ (injective)

$\forall x_1, x_2 \in \mathbb{R}: \quad \phi(x_1 + x_2) = 0.5^{x_1 + x_2} = 0.5^{x_1} \cdot 0.5^{x_2} = \phi x_1 \cdot \phi x_2.$

11. $\forall g \in F: \quad \exists f \in F: \quad f(x) = \int_0^x g(t)\,\mathrm{d}t \Rightarrow \quad (\phi f)(x) = (f')(x) = \left(\int_0^x g(t)\,\mathrm{d}t\right)'(x) = g(x)$

$\forall f_1, f_2 \in F: \quad \phi f_1 = \phi f_2 \Rightarrow \quad \forall x \in \mathbb{R}: \quad f_1'(x) = f_2'(x) \Rightarrow (f_1(0) = f_2(0) = 0) \quad f_1(x) = f_2(x) \Rightarrow \quad f_1 = f_2$

$\forall f_1, f_2 \in F: \quad \phi(f_1 + f_2) = (f_1 + f_2)' = f_1' + f_2' = \phi f_1 + \phi f_2$

12. $f_1 \in F: x \mapsto x^2, \quad f_2 \in F: x \mapsto x^3: \quad f_1'(0) = (2x)(0) = 0, \quad f_2'(0) = (3x^2)(0) = 0$, so ϕ is not injective.

13. $\forall g \in F: \quad \exists f \in F: \quad f = g'$

$\forall f_1, f_2 \in F: \quad \phi f_1 = \phi f_2 \Rightarrow \quad \forall x \in \mathbb{R}: (\phi f)(x) = (\phi f_2)(x) \Rightarrow \quad \forall x \in \mathbb{R}: \int_0^x f_1(t)\,\mathrm{d}t = \int_0^x f_2(t)\,\mathrm{d}t \Rightarrow \quad f_1 = f_2$

$\forall f_1, f_2 \in F: \quad \phi(f_1 + f_2)(x) = \int_0^x (f_1 + f_2)(t)\,\mathrm{d}t = \int_0^x f_1(t)\,\mathrm{d}t + \int_0^x f_2(t)\,\mathrm{d}t = \phi f_1 + \phi f_2$

14. $(\phi f)(x) = \frac{\mathrm{d}}{\mathrm{d}x}\int_0^x f(t)\,\mathrm{d}t = f(x)$

15. $\forall f_1, f_2 \in F: \quad \forall x \in \mathbb{R}: \; \phi(f_1 \cdot f_2)(x) = x \cdot (f_1 \cdot f_2)(x) = x \cdot f_1(x) \cdot f_2(x)$, so ϕ is not an isomorphism.

$(\phi f_1 \cdot \phi f_2)(x) = (\phi f_1)(x) \cdot (\phi f_2)(x) = x \cdot f_1(x) \cdot x \cdot f_2(x)$

16. a. $\forall n_i \in \mathbb{Z}: \quad \exists m_i \in \mathbb{Z}: \quad \phi m_i = n_i \Rightarrow \quad m_i = n_i - 1$

$n_1 * n_2 = \phi m_1 * \phi m_2 = \phi(m_1 m_2) = m_1 m_2 + 1 = (n_1 - 1)(n_2 - 1) + 1$

b. $\forall m_{1,2} \in \mathbb{Z}: \quad \phi(m_1 * m_2) = \phi m_1 + \phi m_2 \Rightarrow \quad (m_1 * m_2) + 1 = m_1 + 1 + m_2 + 1 \Rightarrow \quad m_1 * m_2 = m_1 + m_2 + 1$

17. a. $\forall n_i \in \mathbb{Z}: \quad \exists m_i \in \mathbb{Z}: \quad \phi m_i = n_i \Rightarrow \quad m_i + 1 = n_i \Rightarrow \quad m_i = n_i - 1$

$n_1 * n_2 = \phi m_1 * \phi m_2 = \phi(m_1 \cdot m_2) = m_1 m_2 + 1 = (n_1 - 1)(n_2 - 1) + 1$

b. $\forall m_{1,2} \in \mathbb{Z}: \phi(m_1 * m_2) = \phi m_1 \cdot \phi m_2 \Rightarrow \quad (m_1 * m_2) + 1 = (m_1 + 1)(m_2 + 1) \Rightarrow \quad m_1 * m_2 = (m_1 + 1)(m_2 + 1) - 1.$

18. a. $\forall y_i \in \mathbb{Q}: \quad \exists x_i \in \mathbb{Q}: \quad \phi x_i = y_i \Rightarrow \quad 3x_i - 1 = y_i \Rightarrow \quad 3x_i = y_i + 1$

$y_1 * y_2 = \phi x_1 * \phi x_2 = \phi(x_1 + x_2) = 3(x_1 + x_2) - 1 = (y_1 + 1) + (y_2 + 1) - 1 = y_1 + y_2 + 1$

b. $\forall x_1, x_2 \in \mathbb{Q}: \quad \phi(x_1 * x_2) = \phi x_1 + \phi x_2 \Rightarrow \quad 3(x_1 * x_2) - 1 = (3x_1 - 1) + (3x_2 - 1) \Rightarrow$

$3(x_1 * x_2) = 3x_1 + 3x_2 - 1 \Rightarrow \quad x_1 * x_2 = x_1 + x_2 + \tfrac{1}{3}$

19. a. $\forall y_i \in \mathbb{Q}: \quad \exists x_i \in \mathbb{Q}: \quad \phi x_i = y_i \Rightarrow \quad 3x_i - 1 = y_i \Rightarrow \quad 3x_i = y_i + 1$

$y_1 * y_2 = \phi x_1 * \phi x_2 = \phi(x_1 x_2) = 3x_1 x_2 - 1 = (y_1 + 1)(y_2 + 1) - 1$

b. $\forall x_1, x_2 \in \mathbb{Q}: \quad \phi(x_1 * x_2) = \phi x_1 * \phi x_2 \Rightarrow \quad 3(x_1 * x_2) - 1 = (3x_1 - 1)(3x_2 - 1) \Rightarrow$

$3(x_1 * x_2) = (3x_1 - 1)(3x_2 - 1) + 1 \Rightarrow \quad x_1 * x_2 = (x_1 - \tfrac{1}{3})(x_2 - \tfrac{1}{3}) + \tfrac{1}{3}$

20. The result of the operands after * then ϕ must be equal to that after ϕ then *.

21. A function $\phi: S \to S'$ is an isomorphism between binary structures $(S, *)$ and $(S', *')$ if and only if

$\forall a, b \in S: \quad \phi(a * b) = \phi a *' \phi b.$

22. Exchange the phrases "is an identity for *" and "for all $s \in S$".

23. An element e_L, e_R is a left, right identity of a binary structure $(S, *)$ if and only if $\forall s \in S: \quad e_L * s = s, \quad s * e_R = s.$ Let

$*$ be defined by the table. Then a and b are both such that $\forall s \in S\colon \quad a * s = s,\ b * s = s$, so left, right identites are not unique. The proof of uniqueness of identity breaks down when applied to left, right identities at the point of the 'role reversal' of the two identities.

*	a	b
a	a	b
b	a	b

24. Let e_L, e_R be a left, right identity of a binary structure $(S,*)$. Then

$$\left.\begin{array}{l}\forall s \in S\colon \quad e_L * s = s \Rightarrow \quad e_L * e_R = e_R \\ \forall s \in S\colon \quad s * e_R = s \Rightarrow \quad e_L * e_R = e_L\end{array}\right\} \Rightarrow \quad e_L = e_R$$

25. $$\forall s_1', s_2' \in S'\colon \quad \begin{cases} \phi\left(\phi' s_1' * \phi' s_2'\right) \overset{\phi\text{ isomorphism}}{=} \phi\phi' s_1' * \phi\phi' s_2' \overset{\phi\text{ invertible}}{=} s_1' * s_2' \\ \phi'\left(s_1' * s_2'\right) = \phi'\phi\left(\phi' s_1' * \phi' s_2'\right) \overset{\phi\text{ invertible}}{=} \phi' s_1' * \phi' s_2' \end{cases}$$, so ϕ' is an isomorphism.

26. $$\forall s_1, s_2 \in S\colon \quad (\psi \circ \phi)(s_1 * s_2) = \psi\left(\phi(s_1 * s_2)\right) \overset{\phi\text{ isomorph}}{=} \psi\left(\phi s_1 *' \phi s_2\right) \overset{\psi\text{ isomorph}}{=} \psi(\phi s_1) *'' \psi(\phi s_2) = (\psi \circ \phi) s_1 *'' (\psi \circ \phi) s_2$$

27. reflexive: $(S,*) \cong (S,*)$ by $I\colon S \to S\colon s \mapsto s$.

symmetric: $(S,*) \cong (S',*')$ by $\phi\colon S \to S'$. Then, by Exercise 25 $(S',*') \cong (S,*)$ by ϕ^{inv}.

transitive: If $(S,*) \overset{\phi}{\cong} (S',*')$, $\quad (S',*') \overset{\psi}{\cong} (S'',*'')$, then by Exercise 26, $(S,*) \overset{\psi\circ\phi}{\cong} (S'',*'')$.

28. Let $*$ be commutative on S, and let ϕ be an isomorphism $(S,*) \overset{\phi}{\cong} (S',*')$. So,

$\forall s_i' \in S'\colon \quad \exists s_i \in S\colon \quad \phi s_i = s_i'\colon \quad \phi s_1 *' \phi s_2 \overset{\phi\text{ isomorphism}}{=} \phi(s_1 * s_2) \overset{*\text{ commutative}}{=} \phi(s_2 * s_1) \overset{\phi\text{ isomorphism}}{=} \phi s_2 * \phi s_1$, $*'$ is commutative on S'.

29. Let $*$ be associative on S, and $\phi\colon (S,*) \cong (S',*')$, and $\forall s_i' \in S'\colon \quad \exists s_i \in S\colon \quad \phi s_i = s_i'$. Then

$$\begin{aligned} s_1' *' \left(s_2' *' s_3'\right) &= \phi s_1 *' (\phi s_2 *' \phi s_3) \overset{\phi\text{ isomorph}}{=} \phi s_1 *' \phi(s_2 * s_3) \overset{\phi\text{ isomorph}}{=} \phi\left(s_1 * (s_2 * s_3)\right) \\ &= \phi\left((s_1 * s_2) * s_3\right) \overset{\phi\text{ isomorph}}{=} \phi(s_1 * s_2) *' \phi s_3 \overset{\phi\text{ isomorph}}{=} (\phi s_1 *' \phi s_2) *' \phi s_3 = \left(s_1' * s_2'\right) * s_3' \end{aligned}.$$

30. $\forall c' \in S'\colon \quad \exists c \in S\colon \quad \phi c = c',\ \exists x \in S\colon \quad x * x = c \Rightarrow \quad c' = \phi c = \phi(x * x) = \phi x * \phi x$, so $x' * x' = c'$ has a solution $x' = \phi x \in S$.

31. Let $b \in S\colon \quad b * b \in S$. Then $\exists b' = \phi b \in S'\colon \quad b' = \phi b = \phi(b * b) = \phi b * \phi b = b' * b'$.

32? Let $\phi\colon \mathbb{C} \to H\colon a + bi,\ a,b \in R\colon \quad \mapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, and let $v, w \in \mathbb{C}; \quad v = v' + iv'',\ w = w' + iw'',\ v', v'', w', w'' \in \mathbb{R}$.

a. $$\phi(v + w) = \phi\left((v' + iv'') + (w' + iw'')\right) = \phi\left((v' + w') + i(v'' + w'')\right) = \begin{bmatrix} v' + w' & -(v'' + w'') \\ v'' + w'' & v' + w' \end{bmatrix} = \begin{bmatrix} v' & -v'' \\ v' & v'' \end{bmatrix} + \begin{bmatrix} w' & -w'' \\ w'' & w' \end{bmatrix}$$

$$= \phi(v' + iv'') + \phi(w' + iw'') = \phi v + \phi w$$

b. $$\phi(v \cdot w) = \phi\left((v' + iv'') \cdot (w' + iw'')\right) = \phi\left(v'w' - v''w'' + i(v'w'' + v''w')\right)$$

$$= \begin{bmatrix} v'w' - v''w'' & -(v'w'' + v''w') \\ v'w'' + v''w' & v'w' - v''w'' \end{bmatrix} = \begin{bmatrix} v'w' - v''w'' & v'w'' - v''w' \\ v''w' + v''w' & -v''w'' + v'w' \end{bmatrix} = \begin{bmatrix} v' & -v'' \\ v'' & v' \end{bmatrix} \cdot \begin{bmatrix} w' & -w'' \\ w'' & w' \end{bmatrix}$$

$$= \phi(v' + iv'') + \phi(w' + iw'') = \phi v \cdot \phi w$$

33. The two isomorphisms possible are the identity and $\phi\!:\!(a,b)\mapsto(b,a)$, so the equivalence classes have either one or two elements. Calculate the number of equivalence classes with one element— these are the ones where ϕ coincides with the identity:

$$\begin{cases} C=F', F=C' \\ E=D', D=E' \end{cases} \Rightarrow \quad \begin{cases} C=F' \\ D=E' \end{cases}$$, which corresponds to the four tables where $(C,D)\in\{(a,a),(a,b),(b,a),(b,b)\}$. So there are $4+\dfrac{16-4}{2}=4+6=10$ equivalence classes.

	a	b
a	C	D
b	E	F

	b	a
b	C'	D'
a	E'	F'

	b	a
a	E'	F'
b	C'	D'

	a	b
a	F'	E'
b	D'	C'

§1.3 Groups

1. $\mathbb{Z}$ is closed under $*$.

G1. $\forall a,b,c\in\mathbb{Z}:\quad (a*b)*c=(ab)*c=(ab)c=a(bc)=a*(bc)=a*(b*c)$.

G2. $\forall a\in\mathbb{Z}:\quad 1*a=1\cdot a=a,\quad a*1=a\cdot 1=a$.

G3. $\forall a\in\mathbb{Z}:\quad \nexists a'\in\mathbb{Z}:\quad a*a'=aa'=1\Rightarrow\quad a'=\dfrac{1}{a}$.

2. $\forall a,b\in 2\mathbb{Z}:\quad \exists m,n\in\mathbb{Z}:\quad a=2m, b=2n\Rightarrow\quad a*b=a+b=2m+2n=2(m+n), m+n\in\mathbb{Z}$, so $2\mathbb{Z}$ is closed under $*$.

G1. $\forall a,b,c\in 2\mathbb{Z}:\quad (a*b)*c=(a+b)+c=a+(b+c)=a*(b*c)$.

G2. $\forall a\in 2\mathbb{Z}:\quad a+0=0+a=a$.

G3. $\forall a\in 2\mathbb{Z}:\quad \exists n\in\mathbb{Z}:\quad a=2n$. Let $a'=-a=-(2n)=(-2)n\in 2Z$, so $a'*a=(-a)+a=0,\quad a*a'=a+(-a)=0$.

3. $\forall a,b\in\mathbb{R}^+:\quad a*b=\sqrt{ab}\in\mathbb{R}^+$, so $\mathbb{R}^+$ is closed under $*$.

G1. $\forall a,b,c\in\mathbb{R}^+:\quad (a*b)*c=\left(\sqrt{ab}\right)*c=\sqrt{c\sqrt{ab}}=\sqrt[4]{abc^2}$.

$$a*(b*c)=a*\left(\sqrt{bc}\right)=\sqrt{a\sqrt{bc}}=\sqrt[4]{a^2bc}$$

4. $\forall a,b\in\mathbb{Q}:\quad a*b=ab\in\mathbb{Q}$, so $\mathbb{Q}$ is closed under $*$.

G1. $\forall a,b,c\in\mathbb{Q}:\quad (a*b)*c=(ab)*c=(ab)c=a(bc)=a*(bc)=a*(b*c)$.

G2. $\forall a\in\mathbb{Q}:\quad 1*a=1\cdot a=a,\quad a*1=a\cdot 1=a$.

G3. $\forall a\in\mathbb{Q}:\quad \nexists a'\in\mathbb{Q}:\quad 0\cdot a'=1$

5. $\forall a,b\in\mathbb{R}^+:\quad a*b=a/b\in\mathbb{R}^+$, so $\mathbb{R}^+$ is closed under $*$.

G1. $\forall a,b,c\in\mathbb{R}^+:\quad (a*b)*c=(a/b)/c=a/(bc)$.

$$a*(b*c)=a/(b/c)=ac/b$$

6. $\forall a,b\in\mathbb{C}:\quad a*b=|ab|\in\mathbb{C}$, so $\mathbb{C}$ is closed under $*$.

G1. $\forall a,b,c\in\mathbb{C}:\quad a*(b*c)=a*|bc|=\big|a\cdot|bc|\big|=|abc|$.

$$(a*b)*c=|ab|*c=\big||ab|\cdot c\big|=|abc|$$

G2. $\forall a\in\mathbb{C}:\quad \nexists e\in\mathbb{C}:\quad i*e=|ie|=i$.

7. $\forall a,b\in\{0,\ldots,999\}:\quad a*b=(a+b)\bmod 1000\in\{0,\ldots,999\}$, so the set is closed under $*$.

G1. $\forall a,b,c\in\{0,\ldots,999\}:$

$$\begin{aligned}(a*b)*c&=\big((a+b)\bmod 1000+c\big)\bmod 1000=(a+b+c)\bmod 1000\\ a*(b*c)&=\big(a+(b+c)\bmod 1000\big)\bmod 1000=(a+b+c)\bmod 1000\end{aligned}.$$

G2. $\forall a \in \{0,\ldots,999\}$: $\begin{array}{l} 0 * a = (0+a) \bmod 1000 = a \bmod 1000 = a \\ a * 0 = (a+0) \bmod 1000 = a \bmod 1000 = a \end{array}$.

G3. $\forall a \in \{0,\ldots,999\}$: $\exists a' = (-a) \bmod 1000$: $\begin{cases} a * a' = (a + (-a)) \bmod 1000 = 0 \bmod 1000 = 0 \\ a' * a = ((-a) + a) \bmod 1000 = 0 \bmod 1000 = 0 \end{cases}$.

8. $U = \{e^{i\theta}\}_{\theta \in \mathbb{R}}$

$\forall x,y \in U: \quad \exists \theta,\psi \in \mathbb{R}: \quad x = e^{i\theta}, y = e^{i\psi} \Rightarrow \quad x \cdot y = e^{i\theta}e^{i\psi} = e^{i(\theta+\psi)} \in U$, so U is closed under multiplication.

G1. $\forall x,y,z \in U: \quad \exists \theta,\psi,\phi \in \mathbb{R}: \quad x = e^{i\theta}, y = e^{i\psi}, z = e^{i\phi}$

$$(a \cdot b) \cdot c = \left(e^{i\theta} \cdot e^{i\psi}\right) \cdot e^{i\phi} = e^{i\theta} \cdot \left(e^{i\psi} \cdot e^{i\phi}\right) = a \cdot (b \cdot c).$$

G2. $e = 1 = e^{0i} \in U$: $\forall x \in U$: $e \cdot x = x,\ x \cdot e = x$.

G3. $\forall x \in U: \quad \exists \theta \in \mathbb{R}: \quad x = e^{i\theta} \Rightarrow \quad x' = e^{-i\theta} \in U: \begin{array}{l} x \cdot x' = e^{i\theta}e^{-i\theta} = e^0 = 1 = e \\ x' \cdot x = e^{-i\theta}e^{i\theta} = e^0 = 1 = e \end{array}$.

9. $\forall x \in U: \quad \exists \theta \in \mathbb{R}: \quad x = e^{\theta i} \Rightarrow \quad \exists y, y' \in U: \quad y = e^{\frac{1}{2}\theta i}, y' = e^{\left(\frac{1}{2}\theta + \pi\right)i}, y \neq y'$ where $y \cdot y = e^{\theta i} = x$ and $y' \cdot y' = e^{(\theta + 2\pi)i} = e^{\theta i} = x$. So $(U,\cdot)$ has two distinct 'halves' of each of its elements— this is an algebraic property of the group. Now

$\forall x \in \mathbb{R}: \quad \exists y \in \mathbb{R}: \quad y + y = x \Rightarrow \quad y = \frac{1}{2}x$

$\forall x \in \mathbb{R}^*, x < 0: \quad y \cdot y = x \Rightarrow \quad y = \sqrt{x} \Rightarrow \quad y \notin \mathbb{R}^*$

so $(\mathbb{R},+)$ has just exactly one 'half' for each element, and $(\mathbb{R},*)$ has elements with none. So neither of the three groups are isomorphic.

10. a. $\forall a,b \in (n\mathbb{Z},+): \quad \exists l,m \in \mathbb{Z}^+: \quad a = ln,\ b = mn \Rightarrow \quad a + b = (l+m)n \in (n\mathbb{Z},+)$, so the operation is closed.

G1. + is associative.

G2. $0 \in (n\mathbb{Z},+): \quad \forall a \in (n\mathbb{Z},+): \quad 0 + a = a,\ a + 0 = a$.

G3. $\forall a \in (n\mathbb{Z},+) : \exists m \in \mathbb{Z}: a = mn \Rightarrow a' = (-m)n \in (n\mathbb{Z},+) \Rightarrow \quad a + a' = mn + (-m)n = 0, \quad a' + a = (-m)n + mn = 0$.

b. Define isomorphisms by $\forall n \in \mathbb{N}: \quad \phi : (n\mathbb{Z},+) \to (\mathbb{Z},+): \quad nm \mapsto m$. Then

$\forall m \in \mathbb{Z}: \quad nm \in n\mathbb{Z} \Rightarrow \quad \phi(nm) = m$ (surjective)

$\forall m,p \in \mathbb{Z} : \exists m_n, p_n \in \mathbb{Z} : n = m_n n, p = p_n n : \phi m = \phi p \Rightarrow \quad \phi(m_n n) = \phi(p_n n) \Rightarrow \quad m_n = p_n \Rightarrow \quad m = p$ (injective)

$\forall m,p \in \mathbb{Z}: \quad \phi(nm + np) = \phi(n(m+p)) = m + p = \phi(nm) + \phi(np)$

11. The operation is closed, associative, with identity 0, and inverse $-A$.

12. Write these matrices as $[a_i]_{i=0}^{n=1}$, then the operation is closed by $A \cdot B = [a_i b_i]_{i=0}^{n-1}$. Also

G1. $(A \cdot B) \cdot C = [a_i b_i]_i \cdot [c_i]_i = [a_i b_i c_i]_i = [a_i]_i \cdot [b_i c_i]_i = A \cdot (B \cdot C)$.

G2. $A + 0 = [a_i]_i + [0]_i = [a_i]_i = A, \quad 0 + A = \ldots = A$.

G3. $\forall A = [a_i]_i$: $\exists A' = -A = [-a_i]_i$: $A + A' = [a_i]_i + [-a_i]_i = [0]_i = 0, \quad A' + A = \ldots = 0$.

13. By the calculations in Exercise 12, the operation is closed, associative, with identity 0, and inverse $-A$.

14. As Exercise 13.

15. In our notation, $A \cdot B = \left[\sum_{k=0}^{n-1} a_{ik} b_{kj} \right]_{i,j=0}^{n-1}$. The elements of A and B under the diagonal $a_{i>j,j} = b_{i>j,j} = 0$ are zero, so the elements of AB under the diagonal are:

$$\left[AB\right]_{i>j,j}=\overset{n-1}{\underset{k=0}{+}}a_{ik}b_{kj}=\left(\overset{j}{\underset{k=0}{+}}\ \overset{i}{\underset{k=j+1}{+}}\ \overset{n-1}{\underset{k=i+1}{+}}\right)a_{ik}b_{kj}=\underset{k\le j<i}{+}0\cdot b_{kj}\underset{j<k\le i}{+}a_{ik}\cdot 0\underset{j<i<k}{+}a_{ik}\cdot 0=0$$

so the operation is closed.

G1. $\left(A\cdot B\right)\cdot C=\left[\overset{n-1}{\underset{k=0}{+}}a_{ik}b_{kj}\right]_{i,j=0}^{n-1}\cdot\left[c_{ij}\right]_{i,j=0}^{n-1}=\left[\overset{n-1}{\underset{i=0}{+}}\left(\overset{n-1}{\underset{k=0}{+}}a_{ik}b_{kl}\right)c_{lj}\right]_{i,j}=\left[\overset{n-1}{\underset{k,l=0}{+}}a_{il}b_{lk}c_{kj}\right]_{i,j=0}^{n-1}$ and

$$A\cdot\left(B\cdot C\right)=\left[a_{ij}\right]_{i,j=0}^{n-1}\left[\overset{n-1}{\underset{k=0}{+}}b_{ik}c_{kj}\right]_{i,j=0}^{n-1}=\left[\overset{n-1}{\underset{l=0}{+}}a_{il}\left(\overset{n-1}{\underset{k=0}{+}}b_{lk}c_{kj}\right)\right]=\left[\overset{n-1}{\underset{k,l=0}{+}}a_{il}b_{lk}c_{kj}\right]_{i,j=0}^{n-1}.$$

G2. $A\cdot I=I\cdot A=A$.

G3. $\left|A\right|=\overset{n-1}{\underset{i=0}{+}}a_{ii}$, so A is not invertible if $A=0$.

16. The operation is closed, associative, with identity 0, and inverse –*A*.

17. The operation is closed, associative, and identity by Exercise 15G2. Since $\left|A\right|=1$, an inverse exists: $A'=A^{-1}\Rightarrow\quad A^{-1}A=AA^{-1}=I$. Is the inverse in the group? Suppose that A^{-1} is not upper-triangular, then by the calculation in Exercise 15, neither is $A^{-1}A=I$, which is a contradiction.

18. $\forall A,B$: $\left|AB\right|=\left|A\right|\cdot\left|B\right|$, so the operation is closed. It is associative, with identity *I*, and the regular matrix inverse.

19. a. $\forall a,b\in\mathbb{R}\setminus\left\{-1\right\}:\quad a*b=a+b+ab\in\mathbb{R};\quad a+b+ab=-1\Rightarrow\quad\left(b+1\right)a=-\left(b+1\right)\Rightarrow\quad b=-1\vee a=-\frac{b+1}{b+1}=-1$, so $a*b\in\mathbb{R}\setminus\left\{-1\right\}$.

b.G1. $\forall a,b,c\in\mathbb{R}\setminus\left\{-1\right\}:\quad\left(a*b\right)*c=\left(a+b+ab\right)*c=\left(a+b+ab\right)+c+\left(a+b+ab\right)c=a+b+c+ab+ac+db+abc$,
$\forall a,b,c\in\mathbb{R}\setminus\left\{-1\right\}:\quad a*\left(b*c\right)=a*\left(b+c+bc\right)=a+\left(b+c+bc\right)+a\left(b+c+bc\right)=a+b+c+ab+ac+bc+abc$.

G2. $\forall a\in\mathbb{R}\setminus\left\{-1\right\}:\quad a*e=a\Rightarrow\quad a+e+ae=a\Rightarrow\quad ae=-e\Rightarrow\quad e=0\vee a=-1\Rightarrow\quad e=0$. Conversely, $0*a=0+a+0a=a$, so 0 is the identity.

G3. $\forall a\in\mathbb{R}\setminus\left\{-1\right\}:\quad a'*a=0\Rightarrow\quad a'+a+a'a=0\Rightarrow\quad\left(1+a\right)a'=-a\Rightarrow\left(a\neq-1\Rightarrow 1+a\neq 0\right)\quad a'=-\frac{a}{a+1}$.

Conversely, $a*a'=a-\frac{a}{a+1}-\frac{a^2}{a+1}=\frac{a\left(a+1\right)}{a+1}-\frac{a-a^2}{a+1}=0$, so a' is the inverse.

c. $2*x*3=7\Rightarrow\quad\left(2+x+2x\right)*3=7\Rightarrow\quad\left(2+x+2x\right)+3+\left(2+x+2x\right)3=7\Rightarrow\quad\ldots\Rightarrow\quad 12x=-4\Rightarrow\quad x=-\tfrac{1}{3}$.

20.

	a	*b*	*c*	*d*
a	*e*	*a*	*b*	*c*
b	*a*	*e*	*c*	*b*
c	*b*	*c*	*e*	*a*
d	*c*	*b*	*a*	*e*

	a	*b*	*c*	*d*
a	*e*	*a*	*b*	*c*
b	*a*	*e*	*c*	*b*
c	*b*	*c*	*a*	*e*
d	*c*	*b*	*e*	*a*

	a	*b*	*c*	*d*
a	*e*	*a*	*b*	*c*
b	*a*	*b*	*c*	*e*
c	*b*	*c*	*e*	*a*
d	*c*	*e*	*a*	*b*

*	*1*	*i*	*-1*	*-i*
1	*1*			
i		*-1*		
-1			*1*	
-i				*-1*

The groups represented by the second and third tables are isomorphic by $\phi\!:\!\left(e,a,b,c\right)\mapsto\left(e,b,a,c\right)$.

a. commutative

b. See fourth table— it is isomorphic to the group represented by the second and third tables.

c. Since the group has four elements, *n* must equal two. The four elements are thus represented by $\begin{bmatrix}1&\\&1\end{bmatrix},\begin{bmatrix}1&\\&-1\end{bmatrix},\begin{bmatrix}-1&\\&1\end{bmatrix},\begin{bmatrix}-1&\\&-1\end{bmatrix}$. Each of these squared equals the identity matrix, so this group must be isomorphic to that represented by the first table.

21. A two-element group must be isomorphic to the one represented by Table 1.3.18. A three-element group must be isomorphic to the one represented by Table 1.3.19.

22. The definition of an inverse depends on that of identity, so G2 must precede G3. So the logically possible orders are G1-G2-G3, G2-G1-G3, and G2-G3-G1.

23. a. ‘associativity’ might be defined; the statement “x = identity” is false; the operation “·” is not defined

b. a group is a set with an operation; ‘associativity’ might be defined; ‘identity’ should be defined; ‘inverse’ should be defined

c. the statement “the binary operation is defined” is redundant; associativity axiom is omitted; ‘identity’ should be defined; ‘inverse’ should be defined, after ‘identity’

d. “a set is called a group” is incorrect, rather a set with an operation; ‘associativity’ might be defined; the statement “an operation is associative under addition” is meaningless, an operation is either associative or not; define what ‘a’ is; “$\{e\}$” is a set, many groups do not have a set as an identity element; define a' as the inverse; define a and a' as elements of the group

24. Name this group S.

S	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

$\forall x \in S$: $e \in S$: $x * e = e * x = x$ (G2)

$\forall x \in S$: $x * x = e$ (G3)

$$\begin{aligned}(e * a) * e = a * e = a\\ e * (a * a) = e * e = e\end{aligned}$$, so G1 is not satisfied.

25. a. false; b. true; c. true; d. false; e. false; f. true, assuming the text is correct; g. by Table 18 and 19, true; h. true (see calculation); i. false, no identity element; j.true.

$$a' * (a * x * b) = a' * c \Rightarrow \quad (a' * a) * x * b = a' * c \Rightarrow \quad e * x * b = a' * c \Rightarrow \quad x * b = a' * c \Rightarrow$$

$$(x * b) = a' * c \Rightarrow \quad (x * b) * b' = (a' * c) * b' \Rightarrow \quad x * (b * b') = a' * c * b' \Rightarrow \quad x * e = a' * c * b' \Rightarrow$$

$$x = a' * c * b'$$

26. $\forall a \in A$: $\exists a' \in A$: $a * a' = e$

$$\phi e = \phi(a * a') = \phi a * \phi(a') \Rightarrow \quad (\phi a)' * \phi e = (\phi a)' * \phi a * \phi(a') \Rightarrow \quad (\phi a)' = \phi(a')$$

27. By contradiction. Since G is finite, there are an odd number of elements in G besides e. Reduce by pairs until there is just one element left.

Take any $a \in G, a \neq e$. If $a * a = e$, we stop; otherwise, $a * a = b \in G, b \neq e \Rightarrow \quad b' = (b)' = (a * a)' \overset{(17)}{=} a' * a'$. If $b' = e$, then $a' * a' = e$ and we can stop; otherwise, $b' \neq e$. If $a' = a$ then $e = a * a' = a * a$, which is a contradiction, so $a' \neq a$, that is, a and a' are distinct elements that do not square to identity.

Continue this process until an appropriate element is found, or there is just one element left; call this element c. Suppose $c * c = d \neq e \Rightarrow \quad c' * c' = d'$. If $d' = d$, then $e = d * d$ and we can stop. If $d' = e$, then $c' * c' = e$, and we can stop. Otherwise $c' * c' = b$ for some b we considered in the reduction process, so $c * c = d = b'$, which is impossible because we already removed b'.

So we must have stopped at some point previous and found an appropriate element.

28. a. For $\forall a, b, c \in \mathbb{R}^*$:

$$(a * b) * c = (|a|b) * c = ||a|b|c = |ab|c$$

$$a * (b * c) = a * (|b|c) = |a| \cdot |b|c = |ab|c$$

b. $1 \in \mathbb{R}^*$: $\forall a \in \mathbb{R}^*$: $1 * a = |1| \cdot a = a$

$$\forall a \in \mathbb{R}^* : \quad \frac{1}{|a|} \in \mathbb{R}^* : \quad a * \frac{1}{|a|} = |a| \cdot \frac{1}{|a|} = 1$$

c. $-1 \in \mathbb{R}^*$: $\nexists a \in \mathbb{R}$: $a * -1 = |a| \cdot -1 = -|a| = 1$, so it is not a group.

d. The group axioms with left identity and inverse, or with right identity and inverse, both define groups; the group axioms with left identity and right inverse do not.

29. $x * x = x \Rightarrow \quad x' * x * x = x' * x \Rightarrow \quad x = e$, and the identity is unique.

30. For $\forall a, b \in G$,

$(a*b)*(a*b) = ((a*b)*a)*b = e \Rightarrow \quad ((a*b)*a)*b*b = e*b \Rightarrow \quad ((a*b)*a)*e = b \Rightarrow \quad (a*b)*a = b \Rightarrow$
$(a*b)*a*a = b*a \Rightarrow \quad (a*b)*e = b*a \Rightarrow \quad a*b = b*a$
so G is commutative.

31. $\forall n \in \mathbb{N}^+$, let $U_n = \{z_i \in \mathrm{C}\}_{\mathrm{i=0}}^{\mathrm{n\text{-}1}}$ be the roots of $z^n = 1$. Then $\forall z_{i,j} \in U_n$: $(z_i \cdot z_j)^n = z_i{}^n \cdot z_j{}^n = 1 \cdot 1 = 1$, so $z_i \cdot z_j \in U_n$ and the set is closed under multiplication.

G1. multiplication is associative

G2. $1 \in U_n$: $\forall z_i \in U_n$: $1 \cdot z_i = z_i \cdot 1 = z_i$.

G3. $\forall z_i \in U_n$: $z_i{}^{-1} \in \mathrm{C}$: $z_i \cdot z_i{}^{-1} = z_i{}^0 = 1$, and $\left(z_i{}^{-1}\right)^n = z_i{}^{-n} = \left(z_i{}^n\right)^{-1} = 1^{-1} = 1$, so $z_i{}^{-1} \in U_n$.

32. $\forall a, b \in G$: $(a*b)^1 = (a*b) = (a)*(b) = (a^1)*(b^1)$

$(a*b)^n = (a^n)*(a^b) \Rightarrow$

$(a*b)^{n+1} = (a*b)^n*(a*b) = (a*b)^n*a*b = (a^n)*(b^n)*a*b \overset{n\text{ times abelian}}{=} (a^n)*a*(b^n)*b = (a^{n+1})*(b^{n+1})$.

33. Let $m = |G|$, and consider the $m+1$ elements $a^0, \ldots, a^m$. Since G has only m elements, $\exists i, j$: $a^i = a^j$. Assume without loss of generality that $i \le j$, so $a^i = a^j = a^i * a^{j-i} \Rightarrow \quad (a')^i * a^i = (a')^i * a^i * a^{j-i} \Rightarrow \quad e = a^{j-i}$.

34. $(a*b)^2 = a^2*b^2 \Rightarrow \quad (a*b)*(a*b) = a*a*b*b \Rightarrow \quad a'*a*b*a*b*a' = a'*a*a*b*b*b' \Rightarrow \quad b*a = a*b$.

35. $(a*b)' = a'*b' \Leftrightarrow \quad a*b*(a*b)' = a*b*(a'*b') \Leftrightarrow \quad e = a*b*a*b' \Leftrightarrow \quad b = a*b*a' \Leftrightarrow \quad b*a = a*b$.

36. $a*b*c = e \Rightarrow \quad b*c = a' \Rightarrow \quad b*c*a = e$.

37. Suppose $x*x' \ne e$, then $x*x'*x \ne e*x \Rightarrow \quad x*e \ne x \Rightarrow \quad x'*x*e \ne x'*x \Rightarrow \quad e*e \ne e \Rightarrow \quad e \ne e$.
Suppose $x*e \ne x$, then $x'*x*e \ne x'*x \Rightarrow \quad e*e \ne e \Rightarrow \quad e \ne e$.

38. Define e by $e*a = a$ for some $a \in G$. Then
$\forall b \in G$: $\exists y \in G$: $a*y = b \Rightarrow \quad e*a = a \Rightarrow \quad e*a*y = a*y \Rightarrow \quad e*b = b$,
so e is a left identity. Also,
$\forall a \in G$: $\exists a' \in G$: $a'*a = e$,
so a' is a left inverse for a. By Exercise 37, G is a group.

39. Let ϕ: $(G,*) \to (G,\cdot)$: $a \mapsto a'$. Then

$\forall a \in (G,\cdot)$: $\exists a' \in (G,\cdot)$: $\phi(a') = (a')' = a$ because $(a')' \cdot a' = e \Rightarrow \quad (a')' \cdot a' \cdot a = a \Rightarrow \quad (a')' = a$, so ϕ is surjective.

$\forall a, b \in (G,*)$: $\phi a = \phi b \Rightarrow \quad a' = b' \Rightarrow \quad a' \cdot a = b' \cdot a \Rightarrow \quad e = b' \cdot a \Rightarrow \quad b \cdot e = b \cdot b' \cdot a \Rightarrow \quad b = a$, so ϕ is injective.

$\forall a, b \in (G,*)$: $\phi(a*b) = (a*b)' = (b \cdot a)' = a' \cdot b' = \phi a \cdot \phi b$, so $(G,*) \cong (G,\cdot)$.

40. $\forall g \in G$: $i_g: G \to G: x \mapsto gxg'$. Then

$\forall x \in G$: $\exists g'xg \in G$: $i_g(g'xg) = gg'xg'g = x$ (surjective)

$\forall x, y \in G$: $i_g x = i_g y \Rightarrow \quad gxg' = gyg' \Rightarrow \quad g'gxg'g = g'gyg'g \Rightarrow \quad x = y$ (injective)

$\forall x, y \in G$: $i_g(xy) = gxyg' = gxeyg' = gxg'gyg' = i_g x \cdot i_g y$,

so $G \cong_{i_g} G$.

41. a. monoid
b. semigroup (ε is the identity element)

§1.4 Subgroups

1. $\forall x,y \in \mathbb{R}: \quad x+y \in \mathbb{R}$ (closed), $e_{\mathrm{R}} = e_{\mathrm{C}} = 0$ (identity), $\forall x \in \mathbb{R}: \quad -x \in \mathbb{R}$ (inverse).

2. $1 \in \mathbb{Q}^+: \quad -1 \notin \mathbb{Q}^+$ (inverse), so not a subgroup.

3. $\forall x,y \in 7\mathbb{Z}: \quad \exists x_7, y_7 \in \mathbb{Z}: \quad x = 7x_7, y = 7y_7 \Rightarrow \quad x+y = 7(x_7+y_7) \in 7\mathbb{Z}$ (closed), $e_{7\mathbb{Z}} = e_{\mathbb{C}} = 0$ (identity), $\forall x \in 7\mathbb{Z}: \quad \exists x_7 \in \mathbb{Z}: \quad -x = (-7)x_7 \Rightarrow \quad -x \in 7\mathbb{Z}$ (inverse).

4. $\forall x,y \in i\mathbb{R}: \quad \exists x_i, y_i \in \mathbb{R}: \quad x = ix_i, y = iy_i \Rightarrow \quad x+y = i(x_i+y_i) \in i\mathbb{R}$ (closed), $e_{i\mathbb{R}} = e_{\mathbb{C}} = 0$ (identity), $\forall x \in i\mathbb{R}: \quad \exists x_i \in \mathbb{R}: \quad x = ix_i \Rightarrow \quad -x = i(-x_i) \in i\mathbb{R}$ (inverse).

5. $\forall x,y \in \pi\mathbb{Q}: \quad \exists x_\pi, y_\pi \in \mathbb{Q}: \quad x = \pi x_\pi, y = \pi y_\pi \Rightarrow \quad x+y = \pi(x_\pi + y_\pi) \in \pi\mathbb{Q}$ (closed), $e_{\pi\mathbb{Q}} = e_{\mathbb{C}} = 0$ (identity), $\forall x \in \pi\mathbb{Q}: \quad \exists x_\pi \in \mathbb{Q}: \quad x = \pi x_\pi \Rightarrow \quad -x = \pi(-x_\pi) \in \pi\mathbb{Q}$ (inverse).

6. $\pi^2 \in \{\pi^n\}_{n\in\mathbb{Z}}, \quad \pi^2 + \pi^2 \notin \{\pi^n\}_{n\in\mathbb{Z}}$ (not closed), so not a subgroup.

7. 1. $0 \notin \mathbb{C}^* \Rightarrow \quad \mathbb{R} \not\subseteq \mathbb{C}^*$

   2. $\forall x,y \in \mathbb{Q}^+: \quad x \cdot y \in \mathbb{Q}^+$ (closed), $e_{\mathbb{Q}^+} = e_{\mathbb{C}} = 1$ (identity), $\forall x \in \mathbb{Q}^+: \quad x^{-1} \in \mathbb{Q}^+$ (inverse)

   3. $e_{\mathbb{C}} = 1 \notin 7\mathbb{Z}$ (identity not in subset), so not a subgroup.

   4. $i \in i\mathbb{R}, \quad i \cdot i = -1 \in i\mathbb{R}$ (not closed), so not a subgroup.

   5. $e_{\mathbb{C}} = 1 \Rightarrow \quad \nexists q \in \mathbb{Q}: \quad q\pi = 1$ (identity), so not a subgroup.

   6. $\forall x,y \in \{\pi^i\}_{i\in\mathbb{Z}}: \quad \exists x_\pi, y_\pi \in \mathbb{Z}: \quad x = \pi^{x_\pi}, y = \pi^{y_\pi} \Rightarrow \quad x \cdot y = \pi^{x_\pi \cdot y_\pi} \in \{\pi^i\}_{i\in\mathbb{Z}}$ (closed), $e_{\mathbb{C}} = 1 = \pi^0 \in \{\pi^i\}_{i\in\mathbb{Z}}$ (identity), $\forall x \in \{\pi^i\}_{i\in\mathbb{Z}}: \quad \exists x_\pi \in \mathbb{Z}: \quad x = \pi^{x_\pi} \Rightarrow \quad x^{-1} = \pi^{-x_\pi} \in \{\pi^i\}_{i\in\mathbb{Z}}$ (inverse).

8. Let $A, B \in \mathrm{GL}(n, \mathrm{R})$: $|A| = |B| = 2 \Rightarrow \quad |A * B| = 4$, so multiplication is not closed on that set.

9. By §1.3.12, the set is closed. The identity is in the set. For all $A = [a_{ii}]_{ii} \Rightarrow \quad A^{-1} = \left[a_{ii}^{-1}\right]_{ii}$ is in the set also.

10. By §1.3.15, the set is closed. The identity is in the set. By $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} = \ldots = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ we see that the inverse of at least one element of the set is itself not in the set.

11. By the argument of Exercise 8, multiplication is not closed on that set.

12. By the argument of Exercise 8, multiplication is closed on that set. The identity has a determinant of one, and so is in the set. Since $|A^{-1}| = 1/|A|$, the inverse is also in the set.

13. Let A, B be orthogonal matrices, then $(AB)^{\mathrm{T}}(AB) = B^{\mathrm{T}}A^{\mathrm{T}}AB = B^{\mathrm{T}}B = I$, so AB is orthogonal. Also, $I^{\mathrm{T}}I = I$ so the identity is orthogonal also. Since the transpose of an orthogonal matrix is its inverse, the inverse is also orthogonal.

14. a. $+1 \in \tilde{F}: \mathbb{R} \to \mathbb{R}: x \mapsto 1, \quad -1 \in \tilde{F}: \mathbb{R} \to \mathbb{R}: x \mapsto -1 \Rightarrow \quad (+1) + (-1) = 0 \notin \tilde{F}$, so the set is not closed under addition.

    b. The question of whether $\tilde{F}$ is a subgroup of itself is answered by whether $\tilde{F}$ is a group.

15. a. $\forall f,g \in G: \quad f+g: \mathbb{R} \to \mathbb{R}: (f+g)1 = f1 + g1 = 0 \Rightarrow \quad f+g \in G$ (closed)

    $0 \in \mathbb{R} \to \mathbb{R}: \quad \forall f \in G: \quad f + 0 \in \mathbb{R} \to \mathbb{R}: x \mapsto (f+0)x = fx + 0(x) = fx \Rightarrow \quad f + 0 = f$ (identity)

    $\forall f \in G: \quad f' \in \mathrm{R} \to \mathrm{R}: x \mapsto -fx \Rightarrow \quad \forall x \in \mathrm{R}: \quad (f+f')x = fx + f'x = fx - fx = 0 \Rightarrow \quad f + f' = 0 \in G$ (inverse)

    b. $\forall f \in G: \quad f(1) = 0 \Rightarrow \quad f \notin \tilde{F}$, so the set is not a subset of $\tilde{F}$.

16. a. Let $f \in \mathbb{R} \to \mathbb{R}: x \mapsto \begin{cases} x = 1: & 1 \\ x \neq 1: & -1 \end{cases} \Rightarrow \quad f \in G$, then $(1+f)0 = 1(0) + f0 = 1 + (-1) = 0 \Rightarrow \quad 1 + f \notin \tilde{F}$, so the set is not closed under addition.

    b. $\forall f,g \in G: \quad \forall x \in \mathbb{R}: \quad \begin{cases} (fg)x = fx \cdot gx \neq 0 \Rightarrow \quad fg \in \tilde{F} \\ (fg)1 = f1 \cdot g1 = 1 \cdot 1 = 1 \end{cases} \Rightarrow \quad fg \in G$ (closed)

    $1 \in G: \quad \forall f \in G: \quad \forall x \in \mathbb{R}: \quad (1f)x = 1(x) \cdot fx = 1 \cdot fx = fx \Rightarrow \quad 1f = f$ (identity)

$\forall f \in G: \quad \exists f' \in \mathbb{R} \to \mathbb{R} : x \mapsto (fx)^{-1} : \quad \forall x \in \mathbb{R}: \quad (ff')x = fx \cdot f'x = fx \cdot (fx)^{-1} = 1 \Rightarrow \quad ff' = 1$

$\forall x \in \mathbb{R}: \quad f'x = (fx)^{-1} \neq 0 \Rightarrow \quad f' \in \tilde{F}$ (inverse).

$f'1 = (f1)^{-1} = 1^{-1} = 1 \Rightarrow \quad f' \in G$

17. a. $1 \in \tilde{F} \Rightarrow \quad 1(0) = 1 \Rightarrow \quad (1+1)0 = 1(0) + 1(0) = 1 + 1 = 2 \Rightarrow \quad 1 + 1 \notin \tilde{F}$, so the set is not closed.

b. $\forall f, g \in \tilde{F}: \quad \forall x \in \mathbb{R}: \quad (fg)x = fx \cdot gx \neq 0 \Rightarrow \quad fg \in \tilde{F}$
$(fg)0 = f(0) \cdot g(0) = 1 \cdot 1 = 1$ (closed)

$1 \in \tilde{F} \Rightarrow \quad 1(0) = 1 : \quad \forall f \in \tilde{F}: \quad \forall x \in \mathbb{R}: \quad (f1)x = fx \cdot 1(x) = fx \Rightarrow \quad f1 = f$ (identity)

$\forall f \in \tilde{F}: \quad \exists f' \in \mathbb{R} \to \mathbb{R} : x \mapsto (fx)^{-1} : \quad \forall x \in \mathbb{R}: \quad (ff')x = fx \cdot f'x = fx \cdot (fx)^{-1} = 1 \Rightarrow \quad ff' = 1$
$f0 = 1 \Rightarrow \quad f'0 = (f0)^{-1} = 1$ (inverse)

18. a. $-1 \in \tilde{F} \Rightarrow \quad (-1)0 = -1 \Rightarrow \quad (-1 + -1)0 = (-1)0 + (-1)0 = -1 + -1 = -2$, so the set is not closed under addition.

b. $\forall f, g \in \tilde{F}$: $\quad (fg)0 = f0 \cdot g0 = -1 \cdot -1 = 1$, so the set is not closed under multiplication.

19. a. Let $\forall a \in \mathbb{R}: \quad f_a \in \mathbb{R} \to \{a\}$. Then

$\forall a, b \in \mathbb{R}: \quad \forall x \in \mathbb{R}: \quad (f_a + f_b)x = f_a x + f_b x = a + b \Rightarrow \quad f_a + f_b = f_{a+b}$ (closed)

$\forall a \in \mathbb{R}: \quad \forall x \in \mathbb{R}: \quad (f_a + f_0)x = f_a x + f_0 x = a + 0 = a \Rightarrow \quad f_a + f_0 = f_a$ (identity)

$\forall a \in \mathbb{R}: f'_a = f_{-a} \Rightarrow \quad \forall x \in \mathbb{R}: (f_a + f'_a)x = (f_a + f_{-a})x = f_a x + f_{-a} x = a + (-a) = 0 \Rightarrow \quad f_a + f'_a = 0$ (inverse)

b. $f_0 \notin \tilde{F}$.

20. See table.

21. a. –50, –25, 0, 25, 50

b. 4, 2, 1, $\frac{1}{2}$, $\frac{1}{4}$

c. $\frac{1}{\pi^2}, \frac{1}{\pi}, 1, \pi, \pi^2$.

22. $$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 \cdot 0 - 1 \cdot -1 & 0 \cdot -1 - 1 \cdot 0 \\ -1 \cdot 0 + 0 \cdot -1 & -1 \cdot -1 + 0 \cdot 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 1 \cdot 0 + 0 \cdot -1 & 1 \cdot -1 + 0 \cdot 0 \\ 0 \cdot 0 + 1 \cdot -1 & 0 \cdot -1 + 1 \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \text{ so}$$

$$\left\langle \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}.$$

23. $$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}_{n=0},$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + n \cdot 0 & 1 \cdot 1 + n \cdot 1 \\ 0 \cdot 1 - 1 \cdot 0 & 0 \cdot 1 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \frac{1}{1} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}_{n=-1},$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{n-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ - & 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + n \cdot 0 & 1 \cdot -1 + n \cdot 1 \\ 0 \cdot 1 + 1 \cdot 0 & 0 \cdot -1 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 & n-1 \\ 0 & 1 \end{bmatrix},$$

so by induction $\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \right\}_{n \in \mathbb{Z}}$.

24. $$\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix}_{n=0},$$

$$\begin{bmatrix}3&0\\0&2\end{bmatrix}^{n+1}=\begin{bmatrix}3&0\\0&2\end{bmatrix}^{n}\begin{bmatrix}3&0\\0&2\end{bmatrix}=\begin{bmatrix}3^n&0\\0&2^n\end{bmatrix}\begin{bmatrix}3&0\\0&2\end{bmatrix}=\begin{bmatrix}3^n\cdot3+0\cdot0&3^n\cdot0+0\cdot2\\0\cdot3+2^n\cdot0&0\cdot0+2^n\cdot2\end{bmatrix}=\begin{bmatrix}3^{n+1}&0\\0&2^{n+1}\end{bmatrix},$$

$$\begin{bmatrix}3&0\\0&2\end{bmatrix}^{-1}=\frac{1}{6}\begin{bmatrix}2&0\\0&3\end{bmatrix}=\begin{bmatrix}3^{-1}&0\\0&2^{-1}\end{bmatrix}=\begin{bmatrix}3^n&0\\0&2^n\end{bmatrix}_{n=-1},$$

$$\begin{bmatrix}3&0\\0&2\end{bmatrix}^{n-1}=\begin{bmatrix}3&0\\0&2\end{bmatrix}^{n}\begin{bmatrix}3&0\\0&2\end{bmatrix}^{-1}=\begin{bmatrix}3^n&0\\0&2^n\end{bmatrix}\begin{bmatrix}3^{-1}&0\\0&2^{-1}\end{bmatrix}=\begin{bmatrix}3^n\cdot3^{-1}+0\cdot0&3^n\cdot0+0\cdot2^{-1}\\3^n\cdot0+2^n\cdot0&0\cdot0+2^n\cdot2^{-1}\end{bmatrix}=\begin{bmatrix}3^{n-1}&0\\0&2^{n-1}\end{bmatrix},$$

so by induction $\left\langle\begin{bmatrix}3&0\\0&2\end{bmatrix}\right\rangle=\left\{\begin{bmatrix}3^n&0\\0&2^n\end{bmatrix}\right\}_{n\in\mathbb{Z}}$.

25. $\begin{bmatrix}0&-2\\-2&0\end{bmatrix}=2\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\Rightarrow\quad\left\langle\begin{bmatrix}0&-2\\-2&0\end{bmatrix}\right\rangle\overset{\text{Exercise 22}}{=}2\cdot\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\right\}.$

26. $G_1=\langle\mathbb{Z},+\rangle=\langle1\rangle$,

$G_2=\langle\mathbb{Q},+\rangle$ is not cyclic,

$G_3=\langle\mathbb{Q}^+,\cdot\rangle$ is not cyclic, because $\forall q\geq1:\quad\forall p\in\mathbb{Q}^+,p>q,p$ prime: $\quad p\notin\langle q\rangle$, and the same argument can be made for numbers of the form $1/q$ when $q\leq1$.

$G_4=\langle6\mathbb{Z},+\rangle=\langle6\rangle$,

$G_5=\left\{6^n\right\}_{n\in\mathbb{Z}}=\langle6\rangle$,

$G_6=\left\{a+b\sqrt{2}\right\}_{a,\,b\in\mathbb{Z}}$ is not cyclic, because $\forall a,b\in\mathbb{Z}:\quad\left\langle a+b\sqrt{2}\right\rangle=\left\{na+nb\sqrt{2}\right\}_{n\in\mathbb{Z}}$, so

$\forall n\in\mathbb{Z}:\quad na+(n+1)b\sqrt{2}\notin\left\langle a+b\sqrt{2}\right\rangle$.

27. $3^0=0,\quad3^1=3,\quad3^2=2,\quad3^3=1,\quad3^4=0\Rightarrow\quad\left|\langle3\rangle\right|=\left|\mathbb{Z}_4\right|=4$.

28. $c^0=e,\quad c^1=c,\quad c^2=e\Rightarrow\quad\left|\langle c\rangle\right|=2$.

29. $U_6=\left\{e^{2\pi ji/6}\right\}_{i=0}^{5}=\left\{e^{\frac{1}{3}\pi ji}\right\}_{i=0}^{5}$, so $\left(e^{\frac{2}{3}\pi i}\right)^0=1,\quad\left(e^{\frac{2}{3}\pi i}\right)^1,\quad\left(e^{\frac{2}{3}\pi i}\right)^2=e^{\frac{4}{3}\pi i},\quad\left(e^{\frac{2}{3}\pi i}\right)^3=e^{\frac{6}{3}\pi i}=e^{2\pi i}=e^0=1\Rightarrow$

$\left|\left\langle e^{\frac{2}{3}\pi i}\right\rangle\right|=3$.

30. $U_5=\left\{e^{2\pi ij/5}\right\}_{j=0}^{4}$, so $\left(e^{\frac{4}{5}\pi i}\right)^0=1,\quad\left(e^{\frac{4}{5}\pi i}\right)^1,\quad\left(e^{\frac{4}{5}\pi i}\right)^2=e^{\frac{8}{5}\pi i},\quad\left(e^{\frac{4}{5}\pi i}\right)^3=e^{\frac{12}{5}\pi i}=e^{\frac{2}{5}\pi i},\quad\left(e^{\frac{4}{5}\pi i}\right)^4=e^{\frac{16}{5}\pi i}=e^{\frac{6}{5}\pi i}\Rightarrow$

$\left|\left\langle e^{\frac{4}{5}\pi i}\right\rangle\right|=\left|U_5\right|=5$.

31. $U_8=\left\{e^{2\pi ij/8}\right\}_{i=0}^{7}=\left\{e^{\frac{1}{4}\pi ij}\right\}_{i=0}^{7}$, so $\left(e^{\frac{3}{2}\pi i}\right)^0=e^0,\quad\left(e^{\frac{3}{2}\pi i}\right)^1=e^{\frac{3}{2}\pi i},\quad\left(e^{\frac{3}{2}\pi i}\right)^2=e^{\frac{2}{2}\pi i},\quad\left(e^{\frac{3}{2}\pi i}\right)^3=e^{\frac{1}{2}\pi i},\left(e^{\frac{3}{2}\pi i}\right)^4=e^0\Rightarrow$

$\left|\left\langle e^{\frac{3}{2}\pi i}\right\rangle\right|=4$.

32. $\left(e^{\frac{5}{4}\pi i}\right)^0=e^0,\quad\left(e^{\frac{5}{4}\pi i}\right)^1=e^{\frac{5}{4}\pi i},\quad\left(e^{\frac{5}{4}\pi i}\right)^2=e^{\frac{2}{4}\pi i},\left(e^{\frac{5}{4}\pi i}\right)^3=e^{\frac{7}{4}\pi i},\left(e^{\frac{5}{4}\pi i}\right)^4=e^{\frac{4}{4}\pi i},\left(e^{\frac{5}{4}\pi i}\right)^5=e^{\frac{1}{4}\pi i},\left(e^{\frac{5}{4}\pi i}\right)^6=e^{\frac{6}{4}\pi i},$

$\left(e^{\frac{5}{4}\pi i}\right)^7=e^{\frac{3}{4}\pi i}\Rightarrow\quad\left|\left\langle e^{\frac{5}{4}\pi i}\right\rangle\right|=\left|U_8\right|=8$.

33. $\begin{bmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{bmatrix}$, $\begin{bmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{bmatrix}^2 = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$, so $\left|\left\langle [\ldots] \right\rangle\right| = 2$.

34. $\begin{bmatrix} & & & 1 \\ & & 1 & \\ 1 & & & \\ & 1 & & \end{bmatrix}$, $\begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$, $\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$, so $\left|\left\langle [\ldots] \right\rangle\right| = 3$.

35. $\begin{bmatrix} & 1 & & \\ & & & 1 \\ & & 1 & \\ 1 & & & \end{bmatrix}$, $\begin{bmatrix} & & & 1 \\ 1 & & & \\ & & 1 & \\ & 1 & & \end{bmatrix}$, $\begin{bmatrix} & 1 & & \\ & & & 1 \\ & & 1 & \\ 1 & & & \end{bmatrix}$, so $\left|\left\langle [\ldots] \right\rangle\right| = 2$.

36. a. See table.

b. $\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0,1,2,3,4,5\} = \mathbb{Z}_6$,

$\langle 2 \rangle = \{0,2,4\} \cong \mathbb{Z}_3$,

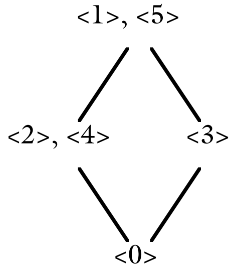
$\langle 3 \rangle = \{0,3\} \cong \mathbb{Z}_2$,

$\langle 4 \rangle = \{0,4,2\} \cong \mathbb{Z}_3$,

$\langle 5 \rangle = \{0,5,4,3,2,1\} = \mathbb{Z}_6$.

c. 1 and 5.

d.



37. Replace "is a subset *H* of *G*" with "is a group on the subset of elements *H* of *G*, with the induced operation from *G*."

38. Ok.

39. a. true (G1); b. false; c. true; d. false (the group itself is the only improper subgroup of itself); e. false; f. false; g. false; h. false; i. true (under addition); j. false.

40. In $\langle \mathbb{R}^+, \cdot \rangle$, $e = 1$, $1^2 = 1$, $(-1)^2 = 1$.

41. $\phi H \subseteq G'$ (subset)

$\forall h_1', h_2' \in \phi H$: $\exists h_1, h_2 \in H$: $\phi h_1 = h_1', \phi h_2 = h_2' \Rightarrow$ $h_1' *' h_2' = \phi h_1 *' \phi h_2 = \phi(h_1 * h_2) \in \phi H$ (closed)

$e_{G'} \overset{(1.2.14)}{=} \phi e_G \overset{(H \subseteq G)}{=} \phi e_H \in \phi H$ (identity)

$\forall h' \in \phi H$: $\exists h^{-1} \in H$: $h^{-1} * h = e_H \Rightarrow$ $\phi(h^{-1} * h) = \phi e \Rightarrow$ $\phi h^{-1} *' \phi h = \phi e \Rightarrow$ $\phi h^{-1} *' h' = e_{H'}$, so $(h')^{-1} = \phi h^{-1}$ (inverse)

42. If G is cyclic, then $\exists g_0 \in G: \quad G = \langle g_0 \rangle \Rightarrow \quad \forall g \in G: \quad \exists m \in \mathbb{Z}: \quad g = {g_0}^m$.

$\forall g' \in G': \quad \exists g \in G: \quad \phi g = g': \quad \exists m \in \mathbb{Z}: \quad g = {g_0}^m \Rightarrow \quad g' = \phi {g_0}^m = (\phi g_0)^m$, so $G' = \langle \phi g_0 \rangle$.

43. Write $HK = \{hk\}_{h \in H, k \in K}$, then

$\forall h_1k_1, h_2k_2 \in HK$: $\left(h_1k_1\right)\left(h_2k_2\right) \overset{\text{abelian}}{=} \left(h_1h_2\right)\left(k_1k_2\right) \overset{h_1h_2 \in H, k_1k_2 \in K}{\in} HK$ (closed)

$e_G = e_G \cdot e_G \overset{H,K \subseteq G}{=} e_H \cdot e_K \in HK$ (identity)

$\forall hk \in HK$: $\exists h^{-1} \in H, k^{-1} \in K$: $h^{-1}k^{-1} \in HK \Rightarrow \left(h^{-1}k^{-1}\right) \cdot \left(hk\right) \overset{\text{abelian}}{=} \left(h^{-1}h\right)\left(k^{-1}k\right) = e_He_K = e_{HK}$, so $\left(hk\right)^{-1} = h^{-1}k^{-1}$ (inverse).

44. $a \in \left\langle H,*\right\rangle \overset{H \subseteq G}{\Rightarrow} a \in \left\langle G,*\right\rangle \Rightarrow a^{-1} \in \left\langle G,*\right\rangle \overset{\text{G3}}{\Rightarrow} a^{=1} \in \left\langle H,*\right\rangle$

$$\left.\begin{array}{l} a *_G a^{-1} \overset{\text{G1}}{\in} \left\langle H,*\right\rangle \\ a *_G a^{-1} = e_G \end{array}\right\} \Rightarrow e_G \in \left\langle H,*\right\rangle, \text{ which proves G2?!}$$

45. $\left(\Rightarrow\right)$ $H \subseteq G \Rightarrow \forall a,b \in H$: $b^{-1} \overset{\text{G3}}{\in} H \Rightarrow ab^{-1} \overset{\text{G1}}{\in} H$

$$\left(\Leftarrow\right) \quad \forall a,b \in H: \quad ab^{-1} \in H \Rightarrow \left\{\begin{array}{l} \forall a \in H: \quad aa^{-1} = e_G \in H\,(\text{G2}) \\ \forall b \in H: \quad eb^{-1} = b^{-1} \in H\,(\text{G3}) \\ \forall a,b \in H: \quad \exists c \in H: \quad c = b^{-1} \Rightarrow \quad ac^{-1} = a\left(b^{-1}\right)^{-1} = ab \in H\,(\text{G1}) \end{array}\right. .$$

46. Let $G = \left\langle g_0 \right\rangle$, so $\forall g \in G: \quad \exists m \in \mathbb{Z}: \quad g = g_0{}^m \Rightarrow \quad g = \left(g_0{}^{-1}\right)^{-m}$, and so a cyclic group must have at least g_0 and its inverse as a generator. If a cyclic group has only one generator, then $g_0 = g_0{}^{-1}$ and $g_0{}^0 = e, \quad g_0{}^1 = g_0, \quad g_0{}^2 = g_0g_0 = g_0g_0{}^{-1} = e$, so $\left|\left\langle g_0 \right\rangle\right| \le 2$.

47. $\forall h_1,h_2 \in H: \quad \left(h_1h_2\right)^2 \overset{\text{commutative}}{=} h_1{}^2h_2{}^2 = e \cdot e = e$ (closed)

$e^2 = e \Rightarrow \quad e \in H$ (identity)

$\forall h \in H: \quad \left(h^{-1}\right)^2 \cdot h^2 \overset{\text{commut.}}{=} \left(h^{-1}h\right)^2 = e^2 = e; \quad \left(h^{-1}\right)^2 = \left(h^{-1}\right)^2 \cdot e = \left(h^{-1}\right)^2 h^2 \overset{\text{commut.}}{=} \left(h^{-1}h\right)^2 = e \Rightarrow \quad \left(h^{-1}\right)^2 \in H$ (inverse).

48. Let $H_{n \in \mathrm{N}^+} = \left\{x \in G\right\}_{x^n = e}$. Then

$\forall h_1,h_2 \in H_n: \quad \left(h_1h_2\right)^n \overset{\text{commut.}}{=} h_1{}^nh_2{}^n = e \cdot e = e$ (closed)

$e^n = e \Rightarrow \quad e \in H_n$ (identity)

$\forall h \in H_n: \quad \left(h^{-1}\right)^n \cdot h^n \overset{\text{commut.}}{=} \left(h^{-1}h\right)^n = e^n = e; \quad \left(h^{-1}\right)^n = \left(h^{-1}\right)^n \cdot e = \left(h^{-1}\right)^n h^n \overset{\text{commut.}}{=} \left(h^{-1}h\right)^n = e^n = e \Rightarrow \quad \left(h^{-1}\right)^n \in H_n$ (inverse).

49. See Exercise 1.3.33.

50. Since $H \ne \varnothing$, $\exists h \in H$. Since H is closed under the operation of G, $\forall m \in \mathbb{N}: \quad h^m \in H$. Since $\left|H\right| \in \mathbb{N}$, $\exists m,n \in \mathbb{N}: \quad h^m = h^n$. Suppose without loss of generality that $m < n$, so $h^m = h^m \cdot h^{n-m}$. Since this is an expression in G also, and since the identity of G is unique, $e_G = h^{n-m} \in H$. Also, $h \cdot h^{n-m-1} = h^{n-m} = e$, so $h^{-1} = h^{n-m-1} \in H$. So H is a subgroup of G.

51. $\forall x,y \in H_a$: $\quad xa = ax, ya = ay \Rightarrow \quad \left(xy\right)a = xay = a\left(xy\right) \Rightarrow \quad xy \in H_a$ (closed)

$ea = a = ae \Rightarrow \quad e \in H_a$ (identity)

$\forall x \in H_a$: $\quad x^{-1}a = x^{-1}ae = x^{-1}axx^{-1} = x^{-1}xax^{-1} = eax^{-1} = ax^{-1} \Rightarrow \quad x^{-1} \in H_a$ (inverse).

52. a. $\forall x,y \in H_s$: $\quad \forall s \in S$: $\quad xs = sx, ys = sy \Rightarrow \quad \left(xy\right)s = xsy = s\left(xy\right) \Rightarrow \quad xy \in H_s$ (closed)

$\forall s \in S\colon \quad es = s = se \Rightarrow \quad e \in H_s$ (identity)

$\forall x \in H_s\colon \quad \forall s \in S\colon \quad x^{-1}s = x^{-1}se = x^{-1}sxx^{-1} = x^{-1}xsx^{-1} = esx^{-1} = sx^{-1} \Rightarrow \quad x^{-1} \in H_s$ (inverse).

b. By definition.

53. $\forall a \in G\colon \quad aa^{-1} = e_G = e_H \in H \Rightarrow \quad a \sim a$

$\forall a, b \in G\colon \quad a \sim b \Rightarrow \quad ab^{-1} \in H \Rightarrow \quad \left(ab^{-1}\right) = ba^{-1} \in H \Rightarrow \quad b \sim a$

$\forall a, b, c \in G\colon \quad a \sim b \wedge b \sim c \Rightarrow \quad ab^{-1}, bc^{-1} \in H \Rightarrow \quad ab^{-1}bc^{-1} = ac^{-1} \in H \Rightarrow \quad a \sim c$.

54. $\forall q, r \in H \cap K\colon \quad q \in H, q \in K, r \in H, r \in K \Rightarrow \quad qr \in H \wedge qr \in K \Rightarrow \quad qr \in H \cap K$ (closed)

$\begin{cases} H \subseteq G \Rightarrow \quad e_H = e_G \in H \\ K \subseteq G \Rightarrow \quad e_K = e_G \in K \end{cases} \Rightarrow \quad e_G \in H \cap K$ (identity)

$\forall q \in H \cap K\colon \quad q^{-1} \in H \wedge q^{-1} \in K \Rightarrow \quad q^{-1} \in H \cap K$ (inverse).

55. $\forall g_1, g_2 \in \langle g_0 \rangle\colon \quad \exists m_1, m_2 \in \mathrm{Z}\colon \quad g_1 = g_0{}^{m_1}, g_2 = g_0{}^{m_2} \Rightarrow \quad g_1 g_2 = g_0{}^{m_1 + m_2} = g_0{}^{m_2 + m_1} = g_0{}^{m_2} g_0{}^{m_1} = g_2 g_1$.

56. This is the case if G is commutative:

$\forall g^n, h^n \in G_n\colon \quad g^n h^n \overset{\text{commutative}}{=} (gh)^n \in G_n$ (closed)

$e = e^n \in G_n$ (identity)

$\forall g^n \in G_n\colon \quad \left(g^{-1}\right)^n \cdot g^n \overset{\text{commutative}}{=} \left(g^{-1}g\right)^n = e^n = e, \quad \left(g^{-1}\right)^n \in G_n$ (inverse).

57. By contradiction: suppose G is not cyclic. If $\nexists g \in G, g \neq e$, then $G = E = \langle e \rangle$, which is a contradiction. So $\exists g \in G, g \neq e$ and by (17), the the nontrivial cyclic group $\langle g \rangle \subseteq G$. But G is not cyclic, so $\exists g' \in G\colon \quad g' \notin \langle g \rangle$, so $\langle g \rangle$ is proper.

§1.5 Cyclic Groups and Generators

1. $42 = 4 \cdot 9 + 6$
2. $-42 = -5 \cdot 9 + 3$
3. $-50 = -7 \cdot 8 + 6$
4. $50 = 6 \cdot 8 + 2$
5. $\gcd(32, 24) = \gcd\left(2^5, 2^3 \cdot 3\right) = 2^3 = 8$.
6. $\gcd(48, 88) = \gcd\left(2^4 \cdot 3, 2^3 \cdot 11\right) = 2^3 = 8$.
7. $\gcd(360, 420) = \gcd\left(2^3 \cdot 3^2 \cdot 5, 2^2 \cdot 3 \cdot 5 \cdot 7\right) = 2^2 \cdot 3 \cdot 5 = 60$.
8. $13 +_{17} 8 = 21 \bmod 17 = 4$.
9. $21 +_{30} 19 = 40 \bmod 30 = 10$.
10. $26 +_{42} 16 = 42 \bmod 42 = 0$.
11. $39 +_{54} 17 = 56 \bmod 54 = 2$.
12. 1, 2, 3, 4: 4 (by relative primes).
13. 1, 3, 5, 7: 4.
14. 1, 5, 7, 11: 4.
15. 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 57, 59: 16.
16. The image of a generator under an isomorphism must be another generator. By Exercise 52, an isomorphism is defined completely by its action on a generator. Therefore, there is one automorphism for each generator that one specific generator could be mapped onto— that is, the number of automorphisms on a cyclic group is the number of generators of that group.
    1: 1.
17. 1, 5: 2.

18. 1, 3, 5, 7: 4.

19. –1, 1: 2.

20. 1, 5, 7, 11: 4.

21. $30/\gcd(25,30) = 30/5 = 6$.

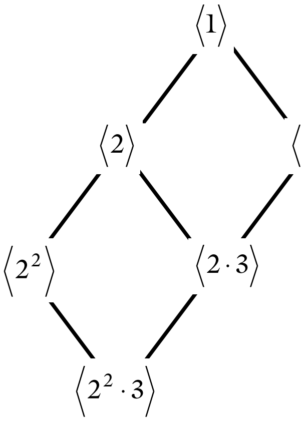
22. $42/\gcd(30,42) = 42/6 = 7$.

23. $\{i, i^2 = -1, i^3 = -i, i^4 = 1\}$: 4.

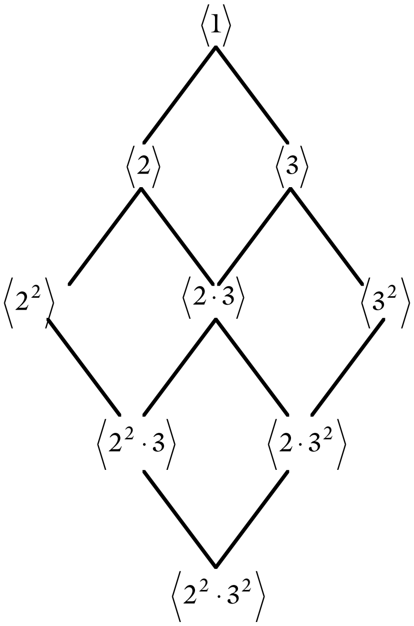
24. $(1+i)/2 = e^{\frac{1}{4}\pi i}, \quad \left|\left\langle e^{\frac{1}{4}\pi i}\right\rangle\right| = 8$.

25. $1+i = \sqrt{2}\cdot e^{\frac{1}{4}\pi i}, \quad \left|\left\langle e^{\frac{1}{4}\pi i}\right\rangle\right| = \aleph_0$.

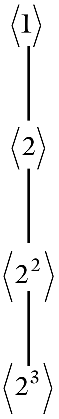
26.



27.


$\langle 1\rangle$
$\langle 2\rangle$
$\langle 3\rangle$
$\langle 2^2\rangle$
$\langle 2\cdot 3\rangle$
$\langle 3^2\rangle$
$\langle 2^2\cdot 3\rangle$
$\langle 2\cdot 3^2\rangle$
$\langle 2^2\cdot 3^2\rangle$

28.



29. $6 = 2\cdot 3$, so the cyclic subgroups are the ones generated by $2^0\cdot 3^0 = 1, \quad 2^1\cdot 3^0 = 2, \quad 2^0\cdot 3^1 = 3, \quad 2^1\cdot 3^1 = 6$.

30. $8 = 2^3 \Rightarrow \quad 2^0 = 2, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8$.

31. $12 = 2^2\cdot 3 \Rightarrow \quad 2^0\cdot 3^0 = 1, \quad 2^1\cdot 3^0 = 2, \quad 2^0\cdot 3^1 = 3, \quad 2^2\cdot 3^0 = 4, \quad 2^1\cdot 3^1 = 6, \quad 2^2\cdot 3^1 = 12$.

32. $20 = 2^2\cdot 5 \Rightarrow \quad 2^0\cdot 5^0 = 1, \quad 2^1\cdot 5^0 = 2, \quad 2^2\cdot 5^0 = 4, \quad 2^0\cdot 5^1 = 5, \quad 2^1\cdot 5^1 = 10, \quad 2^2\cdot 5^1 = 20$.

33. $17 = 17^1 \Rightarrow \quad 17^0 = 1, \quad 17^1 = 17$.

34. $\langle\{2,3\}\rangle = \langle 1\rangle$.

35. $\langle\{4,6\}\rangle = \langle\{2^2, 2\cdot 3\}\rangle = \langle 2\rangle$.

36. $\langle\{8,10\}\rangle = \langle\{2^3, 2\cdot 5\}\rangle = \langle 2\rangle$.

37. $\langle\{12,30\}\rangle = \langle\{2^2\cdot 3, 2\cdot 3\cdot 5\}\rangle = \langle 2\cdot 3\rangle = \langle 6\rangle$.

38. $\langle\{12,42\}\rangle = \langle\{2^2\cdot 3, 2\cdot 3\cdot 7\}\rangle = \langle 2\cdot 3\rangle = \langle 6\rangle$.

39. $\langle\{18,24,39\}\rangle = \langle\{2\cdot 3^2, 2^3\cdot 3, 3\cdot 13\}\rangle = \langle 3\rangle$.

40. Insert the phrase "[if and only if] n is the smallest nonnegative integer such that [$a^n = e$]."

41. Ok.

42. a. true; b. false; c. true; d. false; e. true; f. false (the group of order 3 with the operation that takes the right element); g. true; h. false (G and G' don't even have to be defined on the same set); i. true; j. true.

43. $(\mathbb{Z}_2,+)\times(\mathbb{Z}_2,+)=(\{(0,0),(0,1),(1,0),(1,1)\},+)$.

44. $(\mathbb{C},+)$.

45. E.

46. Every infinite cyclic group is isomorphic to $\mathbb{Z}$, which has two generators.

47. $\mathbb{Z}_5$ has generators 1, 2, 3, 4.

48. $U_4 \cong \mathbb{Z}_4$ which has generators 1, 3, so $\left\{e^{\frac{j}{4}2\pi i}\right\}_{j=1,3}=\left\{e^{\frac{1}{2}\pi i},e^{\frac{3}{2}\pi i}\right\}$.

49. $U_6 \cong \mathbb{Z}_6$: $\left\{e^{\frac{j}{6}2\pi i}\right\}_{j=1,5}=\left\{e^{\frac{1}{3}\pi i},e^{\frac{5}{3}\pi i}\right\}$.

50. $U_8 \cong \mathbb{Z}_8$: $\left\{e^{\frac{j}{8}2\pi i}\right\}_{j=1,3,5,7}=\left\{e^{\frac{1}{4}\pi i},e^{\frac{3}{4}\pi i},e^{\frac{5}{4}\pi i},e^{\frac{7}{4}\pi i}\right\}$.

51. $U_{12} \cong \mathbb{Z}_{12}$: $\left\{e^{\frac{j}{12}2\pi i}\right\}_{j=1,5,7,11}=\left\{e^{\frac{1}{6}\pi i},e^{\frac{5}{6}\pi i},e^{\frac{7}{6}\pi i},e^{\frac{11}{12}\pi i}\right\}$.

52. $\forall x \in G: \quad \exists n \in \mathbb{Z}: \quad x=a^n \Rightarrow \quad \phi x=\phi a^n \overset{\phi \text{ isomorphism}}{=} (\phi a)^n$.

53. $\forall p,q \in S: \quad \exists p_n,p_m,q_n,q_m \in \mathbb{Z}: \quad p=p_n n+p_m m, q=q_n n+q_m m \Rightarrow$
$p+q=(p_n+q_n)n+(p_m+q_m)m, \quad p_n+q_n, p_m+q_m \in \mathbb{Z}$ (closed).
$0=0n+0m \in S$ (identity)
$\forall p \in S: \quad \exists p_n,p_m \in \mathbb{Z}: \quad p=p_n n+p_m m \Rightarrow \quad -p=-(p_n n+p_m m)=(-p_n)n+(-p_m)m \in S$ (inverse).

54. $(ab)^n=e \Rightarrow \quad ab(ab)^{n-2}ab=a(ba)^{n-1}b=e \Rightarrow \quad (ba)^{n-1}b=a^{-1} \Rightarrow \quad (ba)^{n-1}ba=e \Rightarrow \quad (ba)^n=e$. Similarly, $(ba)^{n'}=e \Rightarrow \quad (ab)^{n'}=e$, so $|\langle ba\rangle|=|\langle ab\rangle|$.

55. a. The least common multiple of $r,s \in \mathbb{N}^+$ is the generator of the group $\mathbb{Z}_r \cap \mathbb{Z}_s$ (which exists by Theorem 24). This agrees with the intuitive notion because elements of the intersection must be multiples of both r and s.
b. When $\mathbb{Z}_r \cap \mathbb{Z}_s=\mathbb{Z}_{rs}$.
c.

56. Show that an infinite group has an infinite number of subgroups. If there is a generator a of the group, then it is isomorphic to $\mathbb{Z}$ and thus has an infinite number of subgroups. If it does not have a generator, then …

57. The group $\{0, 1, i, 1+i\}$ under modulo addition is not cyclic, but all its proper subgroups $\langle 0\rangle, \langle 1\rangle, \langle i\rangle, \langle 1+i\rangle$ are.

58. $\mathbb{Z}_n$ is closed under $+_n$. For $\forall r,s,t \in \mathbb{Z}_n$,

$$\begin{aligned}(r+_n s)+_n t&=(((r+s)\bmod n)+t)\bmod n=((r+s)+t)\bmod n\\&=(r+(s+t))\bmod n=(r+(s+t)\bmod n)\bmod n=r+_n(s+_n t)\end{aligned}$$

(associative)
$\forall r \in \mathbb{Z}_n: \quad r+0=r$ (identity)
$\forall r \in \mathbb{Z}_n: \quad r'=\begin{cases}r=0: & 0\\ r\neq 0: & n-r\end{cases} \Rightarrow \quad r+_n r'=\begin{cases}r=0: & 0+_n 0=0\\ r\neq 0: & r+_n(n-r)=n \bmod n=0\end{cases}$ (inverse)

59. $\forall x \in G: \quad a^2=e=xx^{-1}=xa^2x^{-1}=xaax^{-1}=xax^{-1}xax^{-1}=(xax^{-1})^2 \Rightarrow \quad a=xax^{-1} \Rightarrow \quad ax=xa$.

60. $\mathbb{Z}_{pq}$ is generated by all relative primes to pq, that is, to p and q, less than pq. There are $p-1$ divisors by q of pq, and

$q-1$ divisors by p of pq, so there are $(pq-1)-(q-1)-(p-1)$ generators when $p \neq q$ and $(pq-1)-(p-1)$ generators when $p = q$.

61. This again amounts to finding the relative primes to p^r, of which there are $p^{r-1}-1$.

62.

63. $n/\gcd(n,m)$

64. All the proper subgroups of $\mathbb{Z}_p$ are $\langle 1^s = s\rangle$, where $|\langle s\rangle| = p/\gcd(s,p) < p \Rightarrow \quad \gcd(s,p) > 1$, and p has no denominator common with s except 1 if it is prime.

65.

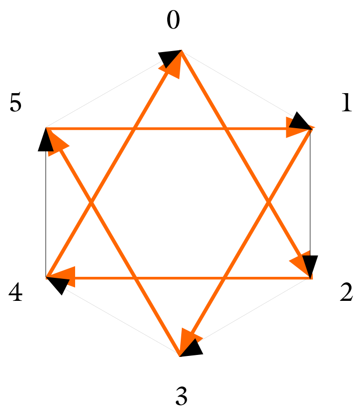
66. Every permutation of edges leads to the same vertex.

67. Not commutative, because $a^3b \cdot b^{-1}a = e, \quad a^3b \cdot ab^{-1} = a^2 \neq e$.

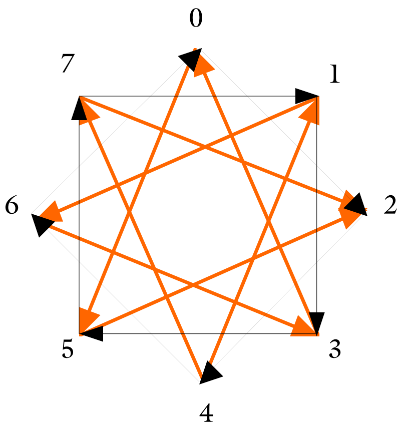
68. Not obvious: one would need to find a path which generates the group.

69. No, because it does not include the identity element.

70.



71.



72. a. A relation is represented by a closed path from the identity element to itself.

b. $b^2 = e, \quad abab = e, \quad a^4 = e, \quad a^2ba^2b = e$.

73. a. $(a^2b)a^3 = a^3b$; b. $(ab)(a^3b) = a^2$; c. $b(a^2b) = a^2$.

74.

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

See table, where $c = ab$.

75.

e	a	b	c	d	f
a	e	c	b	f	d
b	d	e	f	a	c
c	f	a	d	e	b
d	b	f	e	c	a
f	c	d	a	b	e

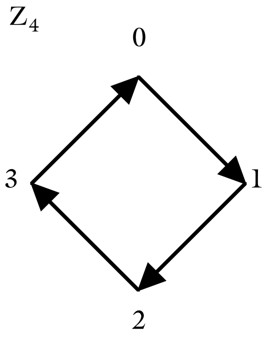
See table, where $c = ab, \quad d = ba, \quad f = aba$.

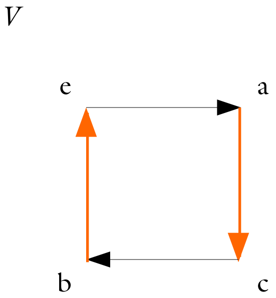
76.

e	a	b	c	d	f
a	c	f	e	d	b
b	d	e	f	a	c
c	e	d	a	f	b
d	f	c	b	e	a
f	b	a	d	c	e

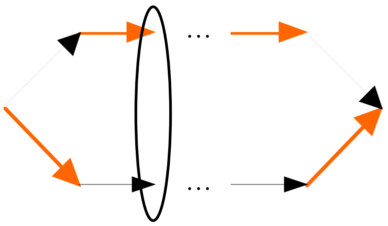
See table, where $c = a^{-1}$, $d = ba$, $f = ba^{-1}$.

77.





78.



(nonabelian)

§2.1 Groups of Permutations

1. $\tau\sigma = (1\ 2\ 3\ 6\ 5\ 4)$

2. $\tau^2\sigma = (2\ 4\ 1\ 5\ 6\ 3)$

3. $\mu\sigma^2 = (3\ 4\ 1\ 6\ 2\ 5)$

4. $\sigma^{-2}\tau = (5\ 1\ 6\ 2\ 4\ 3)$

5. $\sigma^{-1}\tau\sigma = (2\ 6\ 1\ 5\ 4\ 3)$

6. $\sigma^0 = (1\ 2\ 3\ 4\ 5\ 6)$, $\sigma^1 = (3\ 1\ 4\ 5\ 6\ 2)$, $\sigma^2 = (4\ 3\ 5\ 6\ 2\ 1)$, $\sigma^3 = (5\ 4\ 6\ 2\ 1\ 3)$, $\sigma^4 = (6\ 5\ 2\ 1\ 3\ 4)$, $\sigma^5 = (2\ 6\ 1\ 3\ 4\ 5)$,
$\sigma^6 = (1\ 2\ 3\ 4\ 5\ 6) = \sigma^0$, so $|\langle\sigma\rangle| = 6$.

7. $(\tau^2)^0 = (1\ 2\ 3\ 4\ 5\ 6)$, $(\tau^2)^1 = (4\ 3\ 2\ 1\ 5\ 6)$, $(\tau^2)^2 = (1\ 2\ 3\ 4\ 5\ 6) = (\tau^2)^0$, so $|\langle\tau^2\rangle| = 2$.

8. $\sigma^{100} = \sigma^{6\cdot 16+4} = (\sigma^6)^{16}\sigma^4 = \sigma^4 = (6\ 5\ 2\ 1\ 3\ 4)$.

9. $\mu^0 = (1\ 2\ 3\ 4\ 5\ 6)$, $\mu^1 = (5\ 2\ 4\ 3\ 1\ 6)$, $\mu^2 = (1\ 2\ 3\ 4\ 5\ 6)$, so $\mu^{100} = \mu^{2\cdot 50} = (\mu^2)^{50} = e^{50} = e$.

2	3	6	17	$6!$	$\aleph_0$		$\aleph$		
$\langle Z_2,+\rangle$ S_2	$\langle 3Z,+\rangle$		$\langle 17Z,+\rangle$	S_6					
		cyclic			cyclic	acyclic			
		$\langle Z_6,+\rangle$ $\langle(3\ 5\ 4\ 1\ 2)\rangle$			$\langle Z,+\rangle$ $\langle \pi,\cdot\rangle$	$\langle Q,+\rangle$ $\langle Q^*,\cdot\rangle$			
							$\langle R,+\rangle$ $\langle R^+,\cdot\rangle$	$\langle R^*,\cdot\rangle$	$\langle C^*,\cdot\rangle$

10.

11. $O_{1,\sigma} = \{1, 3, 4, 5, 6, 2\}$.

12. $O_{1,\tau} = \{1, 2, 4, 3\}$.

13. $O_{1,\mu} = \{1, 5\}$.

14. $\varepsilon, \rho_1 = \rho, \rho_2 = \rho^2, \mu_1 = \phi, \mu_2 = \rho\phi, \mu_3 = \rho^2\phi$.

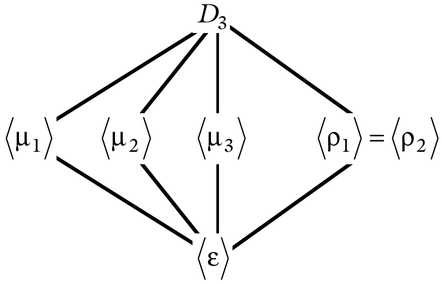
15. $\rho=\rho_1=(2\,3\,4\,1)$, $\phi=\mu_1=(2\,1\,4\,3)$, $\varepsilon=\rho^0$, $\rho_1=\rho^1$, $\rho_2=\rho^2=\rho(2\,3\,4\,1)=(3\,4\,1\,2)$,
$\rho_3=\rho^3=\rho(3\,4\,1\,2)=(4\,1\,2\,3)$, $\phi=\mu_1$, $\phi\rho=\phi(2\,3\,4\,1)=(1\,4\,3\,2)=\delta_2$, $\phi\rho^2=\phi(3\,4\,1\,2)=(4\,3\,2\,1)=\mu_2$,
$\phi\rho^3=\phi(4\,1\,2\,3)=(3\,2\,1\,4)=\delta_1$.

16. $S_4\big|_{\sigma 3=3}\cong S_3 \Rightarrow \left|S_4\big|_{\sigma 3=3}\right|=\left|S_3\right|=3!=6$.

17. $S_5\big|_{\sigma 2=5}\cong S_4 \Rightarrow \left|S_5\big|_{\sigma 2=5}\right|=\left|S_4\right|=4!=24$.

18. a. ${\rho_1}^0=(1\,2\,3)$, ${\rho_1}^1=(2\,3\,1)$, ${\rho_1}^2=(3\,1\,2)$, ${\rho_1}^3=(1\,2\,3)\Rightarrow \langle\rho_1\rangle=\{\varepsilon,\rho_1,\rho_2\}$,
${\rho_2}^0=(1\,2\,3)$, ${\rho_2}^1=(3\,1\,2)$, ${\rho_2}^2=(2\,3\,1)$, ${\rho_2}^3=(1\,2\,3)\Rightarrow \langle\rho_2\rangle=\{\varepsilon,\rho_2,\rho_1\}$,
${\mu_1}^0=\varepsilon$, ${\mu_1}^1=\mu_1$, ${\mu_1}^2=\mu_1(2\,1\,4\,3)=(1\,2\,3\,4)=\varepsilon\Rightarrow \langle\mu_1\rangle=\{\varepsilon,\mu_1\}$.

b. $\langle\mu_2\rangle=\{\varepsilon,\mu_2\}$, $\langle\mu_3\rangle=\{\varepsilon,\mu_3\}$, $\langle\rho_i,\mu_j\rangle_{i=1,\,2;\;j=1,\,2,\,3}=D_3$, $\rho_1\mu_1=\rho_1(1\,3\,2)=(2\,1\,3)=\mu_3$,
${\rho_1}^2\mu_1=\rho_1(2\,1\,3)=(3\,2\,1)=\mu_2$.


D_3
$\langle\mu_1\rangle$
$\langle\mu_2\rangle$
$\langle\mu_3\rangle$
$\langle\rho_1\rangle=\langle\rho_2\rangle$
$\langle\varepsilon\rangle$

19. ${\rho_1}^0=\varepsilon$, ${\rho_1}^1=\rho_1$, ${\rho_1}^2=(3\,4\,1\,2)=\rho_2$, ${\rho_1}^3=\rho_1(3\,4\,1\,2)=(4\,1\,2\,3)=\rho_3$, ${\rho_1}^4=\rho_1(4\,1\,2\,3)=(1\,2\,3\,4)=\varepsilon$,
$\langle\rho_1\rangle=\{\varepsilon,\rho_1,\rho_2,\rho_3\}$;
${\rho_2}^0=\varepsilon$, ${\rho_2}^1=\rho_2$, ${\rho_2}^2=\rho_2(3\,4\,1\,2)=(1\,2\,3\,4)=\varepsilon\Rightarrow \langle\rho_2\rangle=\{\varepsilon,\rho_2\}$;
${\rho_3}^0=\varepsilon$, ${\rho_3}^1=\rho_3$, ${\rho_3}^2=\rho_3(4\,1\,2\,3)=(3\,4\,1\,2)=\rho_2$, ${\rho_3}^3=\rho_3(3\,4\,1\,2)=(2\,3\,4\,1)=\rho_1$,
${\rho_3}^4=\rho_3(2\,3\,4\,1)=(1\,2\,3\,4)=\varepsilon\Rightarrow \langle\rho_3\rangle=\{\varepsilon,\rho_1,\rho_2,\rho_3\}$;
${\mu_1}^0=\varepsilon$, ${\mu_1}^1=\mu_1$, ${\mu_1}^2=\mu_1(2\,1\,4\,3)=(1\,2\,3\,4)=\varepsilon\Rightarrow \langle\mu_1\rangle=\{\varepsilon,\mu_1\}$;
$\langle\mu_2\rangle=\ldots=\{\varepsilon,\mu_2\}$;
${\delta_1}^0=\varepsilon$, ${\delta_1}^1=\delta_1$, ${\delta_1}^2=\delta_1(3\,2\,1\,4)=(1\,2\,3\,4)=\varepsilon\Rightarrow \langle\delta_1\rangle=\{\varepsilon,\delta_1\}$;
$\langle\delta_2\rangle=\ldots=\{\varepsilon,\delta_2\}$

20.
- $\rho^0=(1\,2\,3\,4\,5)$, $\rho^1=(2\,4\,5\,1\,3)$, $\rho^2=(4\,1\,3\,2\,5)$, $\rho^3=(1\,2\,5\,4\,3)$, $\rho^4=(2\,4\,3\,1\,5)$, $\rho^5=(4\,1\,5\,2\,3)$, $\rho^6=(1\,2\,3\,4\,5)=\rho^0$.
- Since $(2\,1\,3)^2=\varepsilon$, $(1\,3\,2)^2=\varepsilon$, there are two distinct elements that square to the identity, while $\langle\rho\rangle$ has only one (ρ^3), so $\langle\rho\rangle\not\cong S_3$.

0	*1*	*2*	*3*	*4*	*5*
1	*2*	*3*	*4*	*5*	*0*
2	*3*	*4*	*5*	*0*	*1*
3	*4*	*5*	*0*	*1*	*2*
4	*5*	*0*	*1*	*2*	*3*
5	*0*	*1*	*2*	*3*	*4*

.

21. a. $\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\2\\3\end{bmatrix}\Rightarrow\ [\ldots]\sim(1\,2\,3)$, $\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}2\\3\\1\end{bmatrix}\Rightarrow\ [\ldots]\sim(2\,3\,1)$, $\begin{bmatrix}&&1\\1&&\\&1&\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\1\\2\end{bmatrix}\Rightarrow\ [\ldots]\sim(3\,1\,2)$,

$\begin{bmatrix}1&&\\&&1\\&1&\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\3\\2\end{bmatrix}\Rightarrow\ [\ldots]\sim(1\,3\,2)$, $\begin{bmatrix}&&1\\&1&\\1&&\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\2\\1\end{bmatrix}\Rightarrow\ [\ldots]\sim(3\,2\,1)$, $\begin{bmatrix}&1&\\1&&\\&&1\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}2\\1\\3\end{bmatrix}\Rightarrow\ [\ldots]\sim(2\,1\,3)$.

Since $(A\cdot B)\mathbf{x}=A(B\mathbf{x})$, the matrices form a group isomorphic to a group of permutations.

b. S_3.

22. $\varepsilon\sim\begin{bmatrix}1&&&\\&1&&\\&&1&\\&&&1\end{bmatrix}$, $\rho_1\sim\begin{bmatrix}&1&&\\&&1&\\&&&1\\1&&&\end{bmatrix}$, $\rho_2\sim\begin{bmatrix}&&1&\\&&&1\\1&&&\\&1&&\end{bmatrix}$, $\rho_3\sim\begin{bmatrix}&&&1\\1&&&\\&1&&\\&&1&\end{bmatrix}$, $\mu_1\sim\begin{bmatrix}&1&&\\1&&&\\&&&1\\&&1&\end{bmatrix}$,

$\mu_2\sim\begin{bmatrix}&&&1\\&&1&\\&1&&\\1&&&\end{bmatrix}$, $\delta_1\sim\begin{bmatrix}&&1&\\&1&&\\1&&&\\&&&1\end{bmatrix}$, $\delta_2\sim\begin{bmatrix}1&&&\\&&&1\\&&1&\\&1&&\end{bmatrix}$.

23. S_2.

24. $S_2\times S_2$.

25. S_4.

26. S_∞.

27. • $\lambda_0=(0+_4)=(0\,1\,2\,3)$, $\lambda_1=(1+_4)=(1\,2\,3\,0)$, $\lambda_2=(2+_4)=(2\,3\,0\,1)$, $\lambda_3=(3+_4)=(3\,0\,1\,2)$, the left regular representation is $\phi:\mathbb{Z}_4\to S_4:x\mapsto\lambda_x$.

•With $S_3=\{\varepsilon,\rho_1,\rho_2,\mu_1,\mu_2,\mu_3\}$:

$\rho_\varepsilon(\varepsilon\,\rho_1\,\rho_2\,\mu_1\,\mu_2\,\mu_3)=(\varepsilon\,\rho_1\,\rho_2\,\mu_1\,\mu_2\,\mu_3)\cdot\varepsilon=(\varepsilon\,\rho_1\,\rho_2\,\mu_1\,\mu_2\,\mu_3)$,

$\rho_{\rho_1}(\varepsilon\,\rho_1\,\rho_2\,\mu_1\,\mu_2\,\mu_3)=(\varepsilon\,\rho_1\,\rho_2\,\mu_1\,\mu_2\,\mu_3)\cdot\rho_1=(\rho_1\,\rho_2\,\varepsilon\,\mu_2\,\mu_3\,\mu_1)$,

et cetera, reading off the columns of Table 2.1.8. Then the right regular representation is ϕ: $S_3\to S_3:\sigma\mapsto\rho_\sigma$.

28. The book definition states “onto”, but this is the same as “to” when a set is mapped to itself.

29. Okay.

30. Permutation.

31. Not surjective for negative numbers.

32. Permutation.

33. Not surjective for nonpositive numbers.

34. $f_5x=x^3-x^2-2x\Rightarrow\ f_5'x=3x^2-2x-2\Rightarrow\ f_5''x=6x-2$. $f_5''x=0\Rightarrow\quad 6x=2\Rightarrow\quad x=\frac{1}{3}$, so

$f_5''0=6\cdot0-2=-2<0$ and $f_5''1=6\cdot1-2=4>0$, and thus f_5 is not injective around $\frac{1}{3}$.

35 a. true; b. false, must map on the same set; c. true; d. true? (book says false); e. true; f. true (by Theorem

1.4.17); g. false, $\left|S_{10}\right| = 10!$; h. false, by Theorem 1.5.1. every cyclic subgroup is commutative, but in Example 2.1.17 S_3 is shown not to be commutative and is thus not cyclic; i. true, any S_n has S_3 as a subgroup and can therefore be neither commutative nor cyclic; j. true

36. S_3 is not commutative, with proper subgroups $\left\langle\left(1\ 2\right)\right\rangle$, $\left\langle\left(1\ 3\right)\right\rangle$, and $\left\langle\left(2\ 3\right)\right\rangle$, each isomorphic to S_2 and commutative.

37. Function composition is associative by 1.1.13. The set has the identity function as an identity element, however the set does not have an inverse for each of its elements. For example, let $a \in A$, then $f_a: x \mapsto a$ has no f_a' such that $f_a \circ f_a' = 1$. This algebraic structure is a monoid.

38. Let $H = \left\{\sigma \in S_A \mid \sigma b = b\right\}$, then $\forall \sigma, \tau \in H$: $\tau^{-1} \in S_A, \tau b = b \Rightarrow \quad \tau^{-1} b = b$, and $\sigma\tau^{-1} \in S_A, \sigma\tau^{-1} b = \sigma b = b \Rightarrow \quad \sigma\tau^{-1} \in H$, so H is a subgroup by Exercise 1.5.45.

39. Let $H = \left\{\sigma \in S_A \mid \sigma b \in B\right\}$. If $B \subset A$ then $\exists a \in A \setminus B$: $\exists \sigma \in H$: $\sigma a = b \Rightarrow \quad \sigma^{-1} b = a \Rightarrow \quad \sigma^{-1} \notin H$, so H is not a subgroup by Theorem 1.4.14.

40. Let $H = \left\{\sigma \in S_A \mid \sigma B \subseteq B\right\}$. $\forall \sigma, \tau \in H$: $\tau B \subseteq B \Rightarrow (\tau \text{ bijective}) \quad \tau B = B \Rightarrow \quad \tau^{-1} B = B$, so $\sigma\tau^{-1} \in S_A$, and $\sigma\tau^{-1} B = \sigma B = B$ and $\sigma\tau^{-1} \in H$.

41. By 40., also a subgroup.

42. A "copy" of an n-gon is any permutation of the vertices of the original in which neighbors of vertices remain neighbors. There are n permutations that leave the orientation unchanged, and another n that reverse it ($n \geq 3$). The first set form a group in itself, because any product of permutations that leave the orientation unchanged itself leaves the orientation unchanged.

43. How many different ways can a cube be rotated? One of its six faces can be rotated upwards, then one of four faces can be rotated leftward, which fixes the rotation. So there are $6 \cdot 4 = 24$ possible rotations. Three subgroups of order four are formed by rotating the cube around its three perpendicular axes, and four subgroups of order three are formed by rotating it around its four diagonal axes.

44. For $\forall S_{n \geq 3}$: $\left(1\ 2\right), \left(1\ 3\right) \in S_n$, and $\left(1\ 2\right)\left(1\ 3\right)\left(1, 2, 3\right) = \left(1\ 2\right)\left(3, 2, 1\right) = \left(2, 3, 1\right)$, $\left(1\ 3\right)\left(1\ 2\right)\left(1, 2, 3\right) = \left(1\ 3\right)\left(2, 1, 3\right) = \left(3, 1, 2\right)$ so the group is not commutative.

45. Let $\sigma \in S_n$: $\forall \gamma \in S_n$: $\sigma\gamma = \gamma\sigma \Rightarrow \quad \sigma = \gamma^{-1}\sigma\gamma$. Suppose $\sigma \neq \iota \Rightarrow \quad \exists i: \sigma i \neq i$. Since $n \geq 3$, $\exists j \neq i, \sigma i$, so define $\gamma = \left(j\ \sigma i\right)$. So $\left(\gamma^{-1}\sigma\gamma\right)i = \left(\gamma^{-1}\sigma\right)i = \gamma^{-1}\left(\sigma i\right) = j$, but $j \neq \sigma i$, so it cannot be that $\sigma \neq \iota$.

46. Suppose $c \in O_{a,\sigma}, O_{b,\sigma}$, then $\exists n_a, n_b \in \mathrm{Z}$: $\sigma^{n_a} a = c, \sigma^{n_b} b = c$. So

$$O_{a,\sigma} = \left\{\sigma^n a\right\}_{n \in \mathrm{Z}} = \left\{\sigma^{n+n_a} a\right\}_{n \in \mathrm{Z}} = \left\{\sigma^n \sigma^{n_a} a\right\}_{n \in \mathrm{Z}} = \left\{\sigma^n c\right\}_{n \in \mathrm{Z}} = \left\{\sigma^n \sigma^{n_b} b\right\}_{n \in \mathrm{Z}} = \left\{\sigma^{n+n_b} b\right\}_{n \in \mathrm{Z}} = \left\{\sigma^n b\right\}_{n \in \mathrm{Z}} = O_{b,\sigma}.$$

47. Number the elements of A by $a_{0 \ldots n-1}$. Generate n permutations $\sigma_i \in S_A$ by $\sigma_i a_j = a_{j +_n i}$. $+_n$ induces n distinct permutations on A. Also, $\forall a_{i,j} \in A$: $j -_n i < n \Rightarrow \quad \sigma_{j -_n i} a_i = a_j$.

48. • If $O_{a,\sigma} = A$ then it is possible to number the elements of A by $a_{0 \ldots n-1}$ such that $\sigma^n a_0 = a_n$. Then $\forall a_{i,j} \in A$: $\sigma^{j-i} a_i = \sigma^{j-i} \sigma^i a_0 = \sigma^j a_0 = a_j$, and $\sigma^{j-i} \in \left\langle\sigma\right\rangle$, so $\left\langle\sigma\right\rangle$ is transitive on A.

• Conversely, let $\left\langle\sigma\right\rangle$ be transitive on A. Then for any given $\forall a \in A$: $\forall a_i \in A$: $\exists \sigma^j \in \left\langle\sigma\right\rangle$: $\sigma^j a = a_i$, so $O_{a,\sigma} = A$.

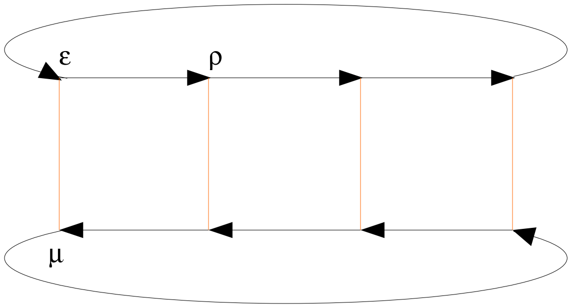
49. a. They will read every product $a * b = c$ as $b * a = c$, and every instance of the associative property of the group $a * \left(b * c\right) = \left(a * b\right) * c$ as an associative property $\left(c * b\right) * a = c * \left(b * a\right)$ of a corresponding, but different, group. Since a group can be defined solely in terms of such expressions, their reversal defines a group also.

b. $\left(a *' b\right) *' c = \left(b * a\right) *' c = c * \left(b * a\right) = \left(c * b\right) * a = a *' \left(c * b\right) = a *' \left(b *' c\right)$ (associativity)
$e *' x = x * e = e$ (left identity)
$a' *' a = a * a' = e$ (left inverse)

50. Show that the right regular representation $\phi: G \to \phi G: g \mapsto \left(\cdot * g\right)$ is an isomorphism. Obviously

$(\cdot * g) = (\cdot * g') \Rightarrow \quad g = g'$ because * is a group operation, so ϕ is an injection, and surjective on ϕG, so a bijection. $\forall g, h \in G$: $\phi(g * h) = (\cdot * (g * h)) = (\cdot * g) * h = (\phi g) * h = \phi h \circ \phi g$, with Exercise 49 shows that $(\phi G, \circ)$ does indeed form a group.

51.



52.

		$T_{\mathbf{x}}s_0$	$T_{\mathbf{x}}s_1$
a.	0	s_0	s_1
b.	1	s_1	s_0
c.	11101	s_0	s_1
d.	010100	s_0	s_1

53.

		$T_{\mathbf{x}}s_0$	$T_{\mathbf{x}}s_1$	$T_{\mathbf{x}}s_2$
a.	0110	s_0	s_0	s_0
b.	0110111	s_2	s_2	s_2
c.	1101	s_1	s_1	s_1
	1	s_1	s_2	s_2
	e	s_0	s_1	s_2

54. $(n+1)^{n+1}$?

55. **yx** is such a string.

56.

T	ε	1
ε	ε	1
1	1	ε

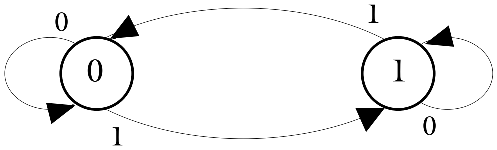
is a group, because it is a monoid with an inverse $T_{\mathbf{x}}^{-1} = T_{\mathbf{x}}$.

57. $T_\varepsilon(s_0\ s_1\ s_2) = (s_0\ s_1\ s_2)$, $T_0(s_0\ s_1\ s_2) = (s_0\ s_0\ s_0)$, $T_1(s_0\ s_1\ s_2) = (s_1\ s_2\ s_2)$, $T_{01}(s_0\ s_1\ s_2) = (s_1\ s_1\ s_1)$, and $T_{11}(s_0\ s_1\ s_2) = (s_2\ s_2\ s_2)$.

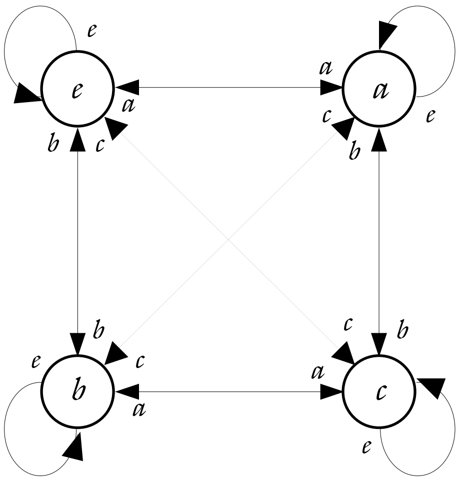
T	ε	0	1	01	11
ε	ε	0	1	01	11
0	0	0	01	01	11
1	1	0	11	01	11
01	01	0	11	01	11
11	11	0	11	01	11

is not a group, because there is no inverse for any $T_{\mathbf{x}}$ except T_ε.

58.



59.



60. The state transition function for an input string $\mathbf{g} = \left(g_0 \dots g_{n-1} \right)$ of the automaton of a finite group G is a function $T_{\mathbf{g}}: G \to G: x \mapsto x \cdot_{i=0}^{n-1} g_i$. Since $\cdot_{i=0}^{n-1} g_i \in G$, T is a permutation of G.

61. isomorphic to G.

§2.2 Orbits, Cycles, and the Alternating Groups

1. $\{1, 5, 2\}, \quad \{3\}, \quad \{4, 6\}$

2. $\{1, 5, 8, 7\}, \quad \{2, 6, 3\}, \quad \{4\}$

3. $\{1, 2, 3, 5, 4\}, \quad \{6\}, \quad \{7, 8\}$

4. $\mathbb{Z}$

5. $\{2i\}_{i \in \mathbb{Z}}, \quad \{2i + 1\}_{i \in \mathbb{Z}}$

6. $\{3i\}_{i \in \mathbb{Z}}, \quad \{3i + 1\}_{i \in \mathbb{Z}}, \quad \{3i + 2\}_{i \in \mathbb{Z}}$

7. $(4\,1\,3\,5\,8\,6\,2\,7)$

8. $(3\,7\,2\,8\,5\,4\,1\,6)$

9. $(5\,4\,3\,7\,8\,6\,2\,1)$

10. $(1\,8)(3\,6\,4)(5\,7) = (1\,8)(3\,4)(3\,6)(5\,7)$

11. $(1\,3\,4)(2\,6)(5\,8\,7) = (1\,4)(1\,3)(2\,6)(5\,7)(5\,8)$

12. $(1\,3\,4\,7\,8\,6\,5\,2) = (1\,2)(1\,5)(1\,6)(1\,8)(1\,7)(1\,4)(1\,3)$

13 a. 4

b. The order of a cycle is equal to the number of elements in its orbit.

c. $\sigma^0 = (\ ), \sigma^1 = (4\,5)(2\,3\,7), \sigma^2 = (2\,7\,3), \sigma^3 = (4\,5), \sigma^4 = (2\,3\,7), \sigma^5 = (4\,5)(2\,7\,3), \sigma^6 = (\ ) = \sigma^0 \Rightarrow \quad |\sigma| = 6,$

$\tau^0 = (\ ), \quad \tau^1 = (1\,4)(3\,5\,7\,8), \quad \tau^2 = (3\,7)(5\,8), \quad \tau^3 = (1\,4)(3\,8\,7\,5), \quad \tau^4 = (\ ) = \tau^0 \Rightarrow \quad |\tau| = 4.$

d. $(1\,8)(3\,6\,4)(5\,7), \quad (3\,4\,6), \quad (1\,8)(5\,7), \quad (3\,6\,4), \quad (1\,8)(3\,4\,6)(5\,7), \quad (\ ) \Rightarrow \quad |\ | = 6,$

$(1\,3\,4)(2\,6)(5\,8\,7), \quad (1\,4\,3)(5\,7\,8), \quad (2\,6), \quad (1\,3\,4)(5\,8\,7), \quad (1\,4\,3)(2\,6)(5\,7\,8), \quad (\ ) \Rightarrow \quad |\ | = 6,$

$(1\,3\,4\,7\,8\,6\,5\,2), \quad (1\,4\,8\,5)(3\,7\,6\,2), \quad (1\,7\,5\,3\,8\,2\,4\,6), \quad \dots \quad \Rightarrow \quad |\ | = 8.$

e. The order of a permutation is equal to the least common multiple of the numbers of elements of the orbits in a decomposition into disjoint cycles.

14. $5 = 2 + 3, \quad \mathrm{lcm}(2, 3) = 6$

15. 6.

16. $7 = 3 + 4, \quad \mathrm{lcm}(3, 4) = 12$

17. $10 = 5 + 3 + 2, \quad \mathrm{lcm}(5, 3, 2) = 30$

18. $15 = 3 + 5 + 7, \quad \mathrm{lcm}(7, 5, 3) = 105$

19. okay

20. [A cycle is a permutation having] at most [one] nontrivial [orbit].

21. For all positive n, A_n [is the] sub[group of all even permutations] of S_n.

22. a. false, but every permutation is a product of disjoint cycles.

b. true

c. true, but it wouldn't have been obvious that a permutation couldn't have been both even and odd

d. false, $\langle(1\ 2\ 3\ 4)\rangle \subseteq S_9$ contains the odd permutation $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$ but none of $(1\ 2\ 3\ 4)^0$, $(1\ 2\ 3\ 4)^1$, $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$, $(1\ 2\ 3\ 4)^3 = (1\ 4\ 3\ 2)$ is a transposition.

e. false, $|A_5| = \frac{1}{2}|S_5| = \frac{1}{2}5! = 60$.

f. false, $S_1 = \{(1)\} = \langle(1)\rangle$.

g. true, $A_3 = \{\varepsilon, \alpha, \alpha^{-1}\}$ where $\alpha = (1\ 2\ 3)$, $\alpha^{-1} = (1\ 3\ 2)$ and the group is commutative:

ε	α	α′
ε	α′	ε
α′	ε	α

h. true

i. true

j. false, (1 2) and (3 4) are both odd permutations but (1 2)(3 4) is even.

23. $\varepsilon = (\ )$, $\rho_1 = (1\ 2\ 3) = (1\ 3)(1\ 2)$, $\rho_2 = (1\ 3\ 2) = (1\ 2)(1\ 3)$ are even, $\mu_1 = (2\ 3)$, $\mu_2 = (1\ 3)$, $\mu_3 = (1\ 2)$ are odd.

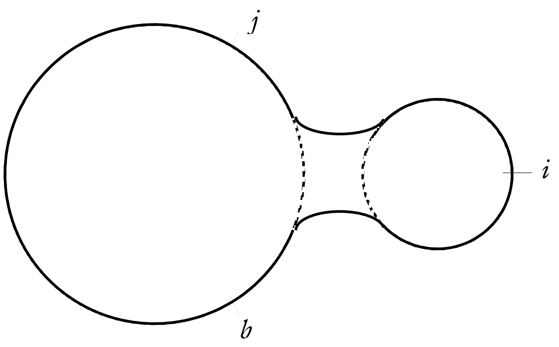
ε	ρ1	ρ2
ρ1	ρ2	ε
ρ2	ε	ρ1

24. a. By induction. For $n = 1$, the only element of $S_1 = \{(1)\}$ can be written as a product of zero transpositions. For $n > 1$, for any $\sigma \in S_n$, the permutation $(\sigma n\ n)\sigma$ does not move n so is a permutation of S_{n-1} and can be written as a product of at most $n - 1$ transpositions. So $(\sigma n\ n)(\sigma n\ n)\sigma = \sigma$ is a product of at most n transpositions.

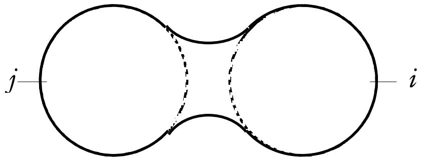
b. If a permutation $\sigma \in S_n$ is not a cycle it consists of at least two cycles. Since by (a) each cycle can be written as a product of at most $n - 1$ transpositions, σ can be written as a product of at most $n - 2$.

c.

25. a. $(i\ j)(b\ j \times\times\times)(i) = (b\ i\ j \times\times\times)$



b. $(i\ j)(j)(i) = (i\ j)$



26. Let $H \subseteq S_n$. Either $\exists \sigma \in H$ where σ is odd, or all the permutations in H are even. In the first case let H_e be the set of even permutations of H, and let $\phi\colon H_e \to H\colon \lambda \mapsto \sigma\lambda$. Since λ is even and σ is odd, λσ must also be odd. If $\exists \lambda, \lambda' \in H_e\colon \sigma\lambda = \sigma\lambda' \Rightarrow \quad \lambda = \lambda'$, so ϕ is a bijection.

§2.3 Cosets and the Theorem of Lagrange

1. $4\mathbb{Z}+0 = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8,\ \ldots\}$,
$4\mathbb{Z}+1 = \{\ldots,\ -7,\ -3,\ 1,\ 5,\ \ldots\}$,
$4\mathbb{Z}+2 = \{\ldots,\ -6,\ -2,\ 2,\ 6,\ \ldots\}$,
$4\mathbb{Z}+3 = \{\ldots,\ -5,\ -1,\ 3,\ 7,\ \ldots\}$.

2. $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$
$4\mathbb{Z}+0 = \{\ldots,\ -4,\ 0,\ 4,\ \ldots\}$, $4\mathbb{Z}+2 = \{\ldots,\ -2,\ 2,\ 6,\ \ldots\}$.

3. $\mathbb{Z}w_{12} = (\{0, \ldots, 11\}, +_{12})$, $\mathbb{Z}_{12} \cap \langle 2 \rangle_{12} = \{0, 2, 4, 6, 8, 10\}$
$\langle 2 \rangle_{12} + 0 = \{0,\ 2,\ 4,\ 6,\ 8,\ 10\}$,
$\langle 2 \rangle_{12} + 1 = \{1,\ 3,\ 5,\ 7,\ 9,\ 11\}$.

4. $\langle 4 \rangle_{12} + 0 = \{0,\ 4,\ 8\}$, $\langle 4 \rangle_{12} + 1 = \{1,\ 5,\ 9\}$, $\langle 4 \rangle_{12} + 2 = \{2,\ 6,\ 10\}$, $\langle 4 \rangle_{12} + 3 = \{3,\ 7,\ 11\}$.

5. $\left\{\langle 18 \rangle_{36} + i\right\}_{i \in \{0,\ \ldots,\ 17\}}$.

6. $\rho_0 \cdot \{\rho_0, \mu_2\} = \{\rho_0, \mu_2\}$,
$\rho_1 \cdot \{\rho_0, \mu_2\} = \{\rho_1, \delta_2\}$,
$\mu_1 \cdot \{\rho_0, \mu_2\} = \{\mu_1, \rho_2\}$,
$\delta_1 \cdot \{\rho_0, \mu_2\} = \{\delta_1, \rho_3\}$.

7. $\{\rho_0, \mu_2\} \cdot \rho_0 = \{\rho_0, \mu_2\}$,
$\{\rho_0, \mu_2\} \cdot \rho_1 = \{\rho_1, \delta_1\}$,
$\{\rho_0, \mu_2\} \cdot \mu_1 = \{\mu_1, \rho_2\}$,
$\{\rho_0, \mu_2\} \cdot \delta_2 = \{\delta_2, \rho_3\}$.
The left and right cosets are not the same.

8. Neither the left nor the right cosets form a group.

	ρ_0	μ_2	ρ_1	δ_2	μ_1	ρ_2	δ_1	ρ_3
ρ_0	ρ_0	μ_2	ρ_1	δ_2	μ_1	ρ_2	δ_1	ρ_3
μ_2	μ_2	ρ_0	δ_1	ρ_3	ρ_2	μ_1	ρ_1	δ_2
ρ_1	ρ_1	δ_2	ρ_2	μ_1	δ_1	ρ_3	μ_2	ρ_0
δ_2	δ_2	ρ_1	μ_2	ρ_0	ρ_3	δ_1	ρ_2	μ_1
μ_1	μ_1	ρ_2	δ_2	ρ_1	ρ_0	μ_2	ρ_3	δ_1
ρ_2	ρ_2	μ_1	ρ_3	δ_1	μ_2	ρ_0	δ_2	ρ_1
δ_1	δ_1	ρ_3	μ_1	ρ_2	ρ_1	δ_2	ρ_0	μ_2
ρ_3	ρ_3	δ_1	ρ_0	μ_2	δ_2	ρ_1	μ_1	ρ_2

	ρ_0	μ_2	ρ_1	δ_1	μ_1	ρ_2	δ_2	ρ_3
ρ_0	ρ_0	μ_2	ρ_1	δ_1	μ_1	ρ_2	δ_2	ρ_3
μ_2	μ_2	ρ_0	δ_1	ρ_1	ρ_2	μ_1	ρ_3	δ_2
ρ_1	ρ_1	δ_2	ρ_2	μ_2	δ_1	ρ_3	μ_1	ρ_0
δ_1	δ_1	ρ_3	μ_1	ρ_0	ρ_1	δ_2	ρ_2	μ_2
μ_1	μ_1	ρ_2	δ_2	ρ_3	ρ_0	μ_2	ρ_1	δ_1
ρ_2	ρ_2	μ_1	ρ_3	δ_2	μ_2	ρ_0	δ_1	ρ_1
δ_2	δ_2	ρ_1	μ_2	ρ_2	ρ_3	δ_1	ρ_0	μ_1
ρ_3	ρ_3	δ_1	ρ_0	μ_1	δ_2	ρ_1	μ_2	ρ_2

9. $\rho_0 \cdot \{\rho_0, \rho_2\} = \{\rho_0, \rho_2\}$,
$\rho_1 \cdot \{\rho_0, \rho_2\} = \{\rho_1, \rho_3\}$,
$\mu_1 \cdot \{\rho_0, \rho_2\} = \{\mu_1, \mu_2\}$,
$\delta_1 \cdot \{\rho_0, \rho_2\} = \{\delta_1, \delta_2\}$.

10. $\{\rho_0, \rho_2\} \cdot \rho_0 = \{\rho_0, \rho_2\}$,
$\{\rho_0, \rho_2\} \cdot \rho_1 = \{\rho_1, \rho_3\}$,
$\{\rho_0, \rho_2\} \cdot \mu_1 = \{\mu_1, \mu_2\}$,
$\{\rho_0, \rho_2\} \cdot \delta_1 = \{\delta_1, \delta_2\}$.
The left and right cosets of this subgroup *are* the same.
So, even a noncommutative group may (must?) have left and right coset partitions that equal, and thus a coset group, if the subgroup is appropriately chosen.

11. This subgroup induces a coset group isomorphic to the Klein 4-group.

	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_2	ρ_2	ρ_0	ρ_3	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_1	ρ_1	ρ_3	ρ_2	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_3	ρ_3	ρ_1	ρ_0	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	μ_2	δ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	μ_1	δ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	δ_2	μ_1	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	δ_1	μ_2	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

V	ε	ρ	μ	δ
ε	ε	ρ	μ	δ
ρ	ρ	ε	δ	μ
μ	μ	δ	ε	ρ
δ	δ	μ	ρ	ε

12. $\langle 3 \rangle_{24} = \{0, 3, \ldots, 21\}$,
$\mathbb{Z}_{24} : \langle 3 \rangle_{24} = |\mathbb{Z}_{24}| / |\langle 3 \rangle_{24}| = 24/8 = 3$.

13. $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$,
$S_3 : \langle \mu_1 \rangle = |S_3| / |\langle \mu_1 \rangle| = 3!/2 = 3$.

14. $D_4 : \langle \mu_1 \rangle = |D_4| / |\langle \mu_1 \rangle| = 8/2 = 4$.

15. $\sigma = \begin{pmatrix} 1 & 2 & 4 & 5 \end{pmatrix}\begin{pmatrix} 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 5 & 4 \end{pmatrix} \Rightarrow \quad |\langle \sigma \rangle| = 5$,
$S_5 : \langle \sigma \rangle = |S_5| / |\langle \sigma \rangle| = 5!/5 = 24$.

16. $\mu = \begin{pmatrix} 1 & 2 & 4 & 5 \end{pmatrix}\begin{pmatrix} 3 & 6 \end{pmatrix} \Rightarrow \quad |\langle \mu \rangle| = 2^2 = 4$,
$S_6 : \langle \mu \rangle = |S_6| / |\langle \mu \rangle| = 6!/4 = 180$.

17. Insert "where $a \in G$".

18. Amend "$H \subseteq G$" (H is a subgroup of G).

19. a. true
b. true
c. true (every subgroup of prime order is cyclic (2.3.11), thus isomorphic to $\mathbb{Z}_n$, and thus commutative)
d. false (the trivial subgroup of any infinite group obviously has left cosets)
e. true ($H = \varepsilon H$)
f. false
g. true (by Theorem 2.2.20)
h. true
i. false (not necessarily if the group is noncommutative)
j. true (because cyclic groups are commutative (1.5.1) and by the remark after 2.3.14)

20. Impossible, by the boxed remark after Example 2.3.3.

21. The improper subgroup of any group G.

22. The trivial subgroup of any group of order 6 such as $\mathbb{Z}_6$.

23. Impossible, since a partition of a set can never produce more cells than the order of the set.

24. Impossible, since by the boxed remark before 2.3.10 the order of each cell of the partition must be equal, and thus equal $6/4 = 1\frac{1}{2}$, and the order of a set must obviously be integral.

25. The relation $\sim_R$ is

- reflexive: $\forall g \in G: \quad g \sim_R g \Leftarrow \quad gg^{-1} = e \in H$,
- symmetric: $\forall g, g' \in G : g \sim_R g' \Rightarrow \quad gg'^{-1} \in H$, and because H is a group, $\left(gg'^{-1}\right)^{-1} = \left(g'^{-1}\right)^{-1} g^{-1} = g'g^{-1} \in H$ so $g' \sim_R g$.
- transitive: $\forall g, g', g'' \in G : g \sim_R g', g' \sim_R g'' \Rightarrow \quad gg'^{-1} \in H \wedge g'g''^{-1} \in H$, and because H is a group, $\left(gg'^{-1}\right) \cdot \left(g'g''^{-1}\right) = gg''^{-1} \in H$, so $g \sim_R g''$,

so it is an equivalence relation.

26. Let $\phi : H \to Hg : h \mapsto hg$. This function is

- surjective: $\left.\begin{array}{r} \forall h \in H : \phi h = hg \in Hg \Rightarrow \quad \phi H \subseteq Hg \\ \forall hg \in Hg \Rightarrow \quad \exists h \in H : \phi h = hg \Rightarrow \quad Hg \subseteq \phi H \end{array}\right\} \Rightarrow \quad \phi H = Hg$,
- injective: $\forall hg, h'g \in Hg : hg = h'g \Rightarrow \quad h = h'$,

so it is bijective.

27. For every left coset defined by some $g \in G$, $\forall gh \in gH \Rightarrow \quad h \in H$, and then because $g^{-1} \in G$, $\left(g^{-1}\right)^{-1} h \left(g^{-1}\right) \in H \Rightarrow \quad ghg^{-1} \in H \Rightarrow \quad \exists h' \in H : ghg^{-1} = h' \Rightarrow \quad gh = h'g \Rightarrow \quad gh \in Hg$, so $gH \subseteq Hg$. Conversely, $Hg \subseteq gH$, so $Hg = gH$.

28. $\forall h \in H, g \in G : hg \in Hg \Rightarrow \quad hg \in gH \Rightarrow \quad \exists h' \in H : hg = gh' \Rightarrow \quad g^{-1}hg = h' \Rightarrow \quad g^{-1}hg \in H$.

♥ 27 and 28 together state that $H \subseteq G$ induces the same left and right coset partition iff $\forall h \in H, g \in G : g^{-1}hg \in H$. We already know from Example 7 that this is equivalent to the existence of a coset group.

29. Counterexample: choose $a = e \Rightarrow \quad \left(H = bH \Rightarrow \quad H = Hb\right) \Rightarrow \quad bH = Hb$, which obviously does not always hold, as in Example 7, where $\rho_1 H \neq H\rho_1$.

30. $\forall a, b \in G : Ha = Hb \Rightarrow \quad \forall h_a \in H : \exists h_b \in H : h_a a = h_b b \Rightarrow \quad {h_b}^{-1} h_a a = b \Rightarrow \quad b \in Ha$.

31. $\forall a, b \in G : aH = bH \Rightarrow \quad \forall h_a \in H : \exists h_b \in H : ah_a = bh_b \Rightarrow \quad h_a = a^{-1}bh_b \Rightarrow \quad h_a{h_b}^{-1} = a^{-1}b \Rightarrow \quad h_a{h_b}^{-1}b^{-1} = a^{-1}$, so $\forall h \in H : ha^{-1} = hh_a{h_b}^{-1}b^{-1} \Rightarrow \quad ha^{-1} \in Hb^{-1} \Rightarrow \quad Ha^{-1} \subseteq Hb^{-1}$. Transposition of '$a$' and '$b$' gives the converse, so that $Ha^{-1} = Hb^{-1}$.

32. Counterexample: choose $a = e \Rightarrow \quad \left(H = bH \Rightarrow \quad H = b^2H\right) \Rightarrow \quad bH = b^2H \Rightarrow \quad H = bH$ which is false if $b \notin H$.

33. The order of any proper subgroup $H \subset G$ must divide the order pq of G, so $|H| \in \{1, p, q\}$ is prime, so by (11) H is cyclic.

34. Let $\phi : \{\gamma H\}_{\gamma \in G} \to \{H\gamma\}_{\gamma \in G} : gH \mapsto Hg^{-1}$, which is:

- surjective:

$$\left.\begin{array}{l} \forall g \in G : gH \in \{\gamma H\}_{\gamma \in G} \Rightarrow \quad \phi(gH) = Hg^{-1} \in \{H\gamma\}_{\gamma \in G} \Rightarrow \quad \phi\left(\{\gamma H\}_{\gamma \in G}\right) \subseteq \{H\gamma\}_{\gamma \in G} \\ \qquad \forall g \in G : Hg \in \{H\gamma\}_{\gamma \in G} \Rightarrow \quad \exists g^{-1} \in G : g^{-1}H \in \{\gamma H\}_{\gamma \in G} \\ \quad \Rightarrow \quad \phi\left(g^{-1}H\right) = H\left(g^{-1}\right)^{-1} = Hg \Rightarrow \quad \phi\left(\{\gamma H\}_{\gamma \in G}\right) \supseteq \{H\gamma\}_{\gamma \in G} \end{array}\right\} \Rightarrow \quad \phi\left(\{\gamma H\}_{\gamma \in G}\right) = \{H\gamma\}_{\gamma \in G},$$

- injective: $\forall g, g' \in G : gH, g'H \in \{\gamma H\}_{\gamma \in G} : \phi(gH) = \phi(g'H) \Rightarrow \quad Hg^{-1} = Hg'^{-1}$, so

$\forall h \in H : \exists h' \in H : h^{-1}g^{-1} = h'g'^{-1} \Rightarrow \quad \left(h^{-1}g^{-1}\right)^{-1} = \left(h'g'^{-1}\right)^{-1} \Rightarrow \quad gh = g'h'^{-1} \Rightarrow \quad gh \in g'H \Rightarrow \quad gH \subseteq g'H$.

Transposition of symbols gives the converse, so $gH \subseteq g'H$.

So the function is bijective, which shows the existence of an isomorphism between the left and right coset partition, and thus (for infinite sets, by definition) their equal size.

35. Suppose there were two elements c, d of order 2, then $\langle c, d\rangle$ would generate a subgroup of order 4 (remebering that the group is commutative):

	e	c	d	cd
e	e	c	d	cd
c	c	$cc = e$	cd	$ccd = d$
d	d	$dc = cd$	$dd = e$	$dcd = ddc = c$
cd	cd	$cdc = ccd = d$	$cdd = c$	$cdcd = cddc = cc = e$

By Lagrange, $|\langle c, d\rangle| = 4$ would have to divide $2n = 4\dfrac{n}{2}$, but $\dfrac{n}{2}$ is not integral.

36. $\forall g \in G : \quad \langle g\rangle \subseteq G$. Since G has no proper subgroups, $\langle g\rangle = G$. If G is of infinite order, then $\langle g^2\rangle \subset \langle g\rangle = G$ which contradicts G not having a proper subgroup, so G must be of finite order. Similarly, if $|\langle g\rangle|$ is divisible by $n > 1$, then $\langle g^n\rangle \subset \langle g\rangle$, again contradicting. So G must be of prime order.

37. We need to show that each of the elements is in fact a left coset of K in G, that every such coset is an element, and that the elements are distinct. So, let $\{a_i\}_{0 \le i < G:H}$ be such that $\{a_iH\}$ is the set of distinct left cosets of H in G, and $\{b_i\}_{0 \le i < H:K}$ such that $\{b_iK\}$ is the set of distinct left cosets of K in H.

- $\forall a_i, b_j \Rightarrow \quad a_ib_j \in G \Rightarrow \quad a_ib_jK$ is a left coset of K in G;
- $\forall g \in G : gK$ is a left coset of K in G, since $\bigcup_i a_iH = G \Rightarrow \quad \exists a_i : g \in a_iH \Rightarrow \quad \exists h \in H : g = a_ih$, and since

$\bigcup_j b_j K = H \Rightarrow \quad \exists b_j : h \in b_j K \Rightarrow \quad \exists k \in K : h = b_j k$, so $gK = a_i b_j k K = a_i b_j K$;

- $\forall a, a' \in \{a_i\};\ b, b' \in \{b_i\} : abK = a'b'K \Rightarrow \quad$ ($a_i H$ are distinct in G) $a = a' \Rightarrow \quad bK = b'K$, so ($b_i K$ are distinct in H) $b = b'$.

So $\bigcup_{i,j} \{a_i b_j K\} = G$ is a distinct left coset partition of G, so $G : K = \left|\{a_i\}_i\right| \cdot \left|\{b_i\}_i\right| = G : H \cdot H : K$.

38. Obviously H is itself one of the left cosets of H in G. Since there is just one other left coset, and since the cosets form a partition of G, the other is $G \setminus H$. The same argument holds for the right coset partition, so the left and right coset partitions are equal.

39. $\langle a \rangle \subseteq G$, so $|\langle a \rangle|$ divides $|G|$, that is $\exists m \in \mathrm{N} : m|\langle a \rangle| = |G|$, so $a^n = a^{|G|} = a^{m|\langle a \rangle|} = e^m = e$.

40. The left cosets of $\mathbb{Z}$ in $(\mathbb{R},+)$ are $\{\chi + \mathbb{Z}\}_{\chi \in \mathbb{R}}$. Then $\forall \chi \in \mathbb{R}$: $\quad \forall x, x' \in \chi + \mathbb{Z} \quad \wedge \quad x, x' \in [0,1[$,

$\Rightarrow \quad |x - x'| = |(x - \chi) - (x' - \chi)| \overset{x-\chi\,,\, x'-\chi \in \mathbb{Z}}{\in} \mathbb{Z}^+$ and $|x - x'| \le |[0,1[| < 1$, so $|x - x'| = 0 \Rightarrow \quad x = x'$.

41. The left cosets of $\langle 2\pi \rangle$ in $(\mathbb{R},+)$ are $\{\chi + \langle 2\pi \rangle\}_{\pi \in \mathbb{R}}$. Then

$\forall \chi \in \mathbb{R}$: $\forall x \in \chi + \langle 2\pi \rangle \Rightarrow \quad \exists n \in \mathbb{Z} : x = \chi + n \cdot 2\pi \Rightarrow \quad \sin x = \sin(\chi + n \cdot 2\pi) = \sin \chi$, so it does indeed make sense to write the sine function as $\sin : \{\chi + \langle 2\pi \rangle\}_{\chi \in \mathbb{R}} \to [-1,+1]$.

42. a. The relation ~ is an equivalence relation because it is:

- reflexive: $a \sim a \quad \Leftarrow \exists h \in H, k \in K : a = hak \quad \Leftarrow a = a;\ h, k = e$;
- symmetric: $\forall a, b \in G : a \sim b \Rightarrow \quad \exists h \in H, k \in K : a = hbk \Rightarrow \quad h^{-1} a k^{-1} = b, h^{-1} \in H, k^{-1} \in K \Rightarrow \quad b \sim a$;
- transitive: $\forall a, b, c : a \sim b,\ b \sim c \Rightarrow \quad \exists h, h' \in H;\ k, k' \in K : a = hbk,\ b = h'ck' \Rightarrow \quad a = hh'ck'k,\ hh' \in H,\ k'k \in K$, so $\Rightarrow \quad a \sim c$.

b. $\exists h \in H, k \in K : a = hbk \quad \Leftrightarrow \quad a \in HbK$.

43. a. Prove it is a subgroup because it satisfies the requirements of Theorem 1.4.14:

- $\forall \sigma, \sigma' \in S_{c,c} : \quad (\sigma \circ \sigma')c = \sigma c = c$, so the subset is closed under the operation of S_A;
- The identity permutation e of A certainly has $e(c) = c$, so $e \in S_{c,c}$;
- $\forall \sigma \in S_{c,c} : \quad \sigma^{-1} c = c$, so $\sigma^{-1} \in S_{c,c}$;

so $S_{c,c} \subseteq S_A$.

b. The identity permutation of S_A is not closed in $S_{c,d}$, so again by Theorem 1.4.14, $S_{c,d} \not\subseteq S_A$.

c. $S_{c,d}$ is one of the left cosets $\{\sigma \circ S_{c,c}\}_{\sigma \in S_A}$ of $S_{c,c}$.

44.

45. $\forall n \in \mathrm{N} : \quad \forall i : 0 \le i < n$, i is a generator of exactly one subgroup of $\mathbb{Z}_n$, and conversely, any subgroup of $\mathbb{Z}_n$ must be generated by $i : 0 \le i < n$, so it suffices to enumerate the generators of the subgroups. By Exercise 44, the subgroups of $\mathbb{Z}_n$ are $\{\mathbb{Z}_d\}_{d|n}$, and by Corollary 1.5.18, $\mathbb{Z}_d$ has ϕd generators, so $n = +_{d:\, d|n} \phi d$.

46.

§2.4 Direct Products and Finitely Generated Abelian Groups

1. $\mathbb{Z}_2 \times \mathbb{Z}_4 = \begin{Bmatrix} (0,0) & (0,1) & (0,2) & (0,3) \\ (1,0) & (1,1) & (1,2) & (1,3) \end{Bmatrix}$. The orders are $\begin{Bmatrix} 1 & 4 & 2 & 4 \\ 2 & 4 & 2 & 4 \end{Bmatrix}$. There is no element of order $|\mathbb{Z}_2 \times \mathbb{Z}_4| = 8$, so it is not cyclic.

2. $\mathbb{Z}_3 \times \mathbb{Z}_4 = \begin{Bmatrix} (0,0) & (0,1) & (0,2) & (0,3) \\ (1,0) & (1,1) & (1,2) & (1,3) \\ (2,0) & (2,1) & (2,2) & (2,3) \end{Bmatrix}$. The orders are $\begin{Bmatrix} 1 & 4 & 2 & 4 \\ 3 & 12 & 6 & 12 \\ 3 & 12 & 6 & 12 \end{Bmatrix}$. There are elements of order

$\left|\mathbb{Z}_3 \times \mathbb{Z}_4\right| = 12$, so the group is cyclic.

3. lcm(2, 2) = 2 (by Theorem 9).

4. lcm(3, 5) = 15.

5. lcm(3, 9) = 9.

6. lcm(4, 6, 5) = 60.

7. lcm(4, 2, 5, 3) = 60.

8. $\mathbb{Z}_3 \times \mathbb{Z}_8 \subset \mathbb{Z}_6 \times \mathbb{Z}_8$, $\left|\mathbb{Z}_3 \times \mathbb{Z}_8\right| = 24$ (excepting the nonproper subgroup).

9. $\left\{\left\langle(0,1)\right\rangle, \left\langle(1,0)\right\rangle, \left\langle(1,1)\right\rangle\right\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2$.

10. $\left\{\left\langle(0,0,1)\right\rangle, \left\langle(0,1,0)\right\rangle, \left\langle(0,1,1)\right\rangle, \left\langle(1,0,0)\right\rangle, \left\langle(1,0,1)\right\rangle, \left\langle(1,1,0)\right\rangle, \left\langle(1,1,1)\right\rangle, \right\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

$\left\{(0,0),(0,1),(0,2),(0,3)\right\}$

11. $\left\{(0,0),(1,1),(0,2),(1,3)\right\}$.

$\left\{(0,0),(0,2),(1,0),(1,2)\right\}$

12. $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V \Rightarrow \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_1 \cong V \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong V \end{cases}$, so the subgroups are

$\left\{(0,0,0), \quad (0,1,0), \quad (1,0,0), \quad (1,1,0)\right\}$

$\left\{(0,0,0), \quad (0,0,2), \quad (1,0,0), \quad (1,0,2)\right\}$.

$\left\{(0,0,0), \quad (0,0,2), \quad (0,1,2), \quad (0,1,2)\right\}$

13. $60 = 2^2 \cdot 3 \cdot 5$, so by Corollary 6

$$\mathbb{Z}_{60} \cong \begin{array}{l} \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_{12} \times \mathbb{Z}_5 \\ \mathbb{Z}_{20} \times \mathbb{Z}_3 \\ \mathbb{Z}_{15} \times \mathbb{Z}_4 \end{array} .$$

14. a. 4 ($\left\{0, 18, 12, 6\right\}$).

b. 12 (by Corollary 6, $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$).

c. lcm(3, 4) = 12.

d. $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

e. $2 \cdot 1 \cdot 4 = 8$.

15. $\left\langle\{2,3\}\right\rangle = \left\langle\{1\}\right\rangle = \mathbb{Z}_{12}$. The left cosets are $\bigcup_{i \in \{0\}} \mathbb{Z}_{12} + i$.

16. $\left\langle\{4,6\}\right\rangle = \left\langle\{2\}\right\rangle$. The left cosets are $\bigcup_{i \in \{0,1\}} \left\langle\{2\}\right\rangle + i$.

17. $\left\langle\{8,6,10\}\right\rangle = \left\langle\{2\}\right\rangle$. The left cosets are $\bigcup_{i \in \{0,1\}} \left\langle\{2\}\right\rangle + i$.

18. $\left\langle\{\rho_2, \mu_1\}\right\rangle = \{\rho_0, \rho_2, \mu_1, \mu_2\}$. The left cosets are $\bigcup_{i \in \{\rho_0, \rho_1\}} \left\langle\{\rho_2, \mu_1\}\right\rangle \cdot i$.

19. $\left\langle\{\mu_1, \delta_2\}\right\rangle = \{\rho_0, \mu_1, \delta_2, \rho_1, \rho_3, \delta_1, \mu_2, \rho_2\} = D_4$. The left cosets are $\bigcup_{i \in \{\rho_0\}} \left\langle\{\mu_1, \delta_2\}\right\rangle \cdot i$.

20. $\left\langle\left\{(4,2),(2,3)\right\}\right\rangle = \left\langle(2,3)\right\rangle = \left\langle\left\{(0,0),(2,3),(4,2),(0,1)\right\}\right\rangle = \left\langle\left\{(2,0),(0,1)\right\}\right\rangle$. The left cosets are $\bigcup_{i \in \{(0,0),(1,0)\}} \left\langle\left\{(2,0),(0,1)\right\}\right\rangle \cdot i$.

21. $8 = 2^3$, giving $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_8$.

22. $16 = 2^4$, giving $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_8 \times \mathbb{Z}_2, \quad \mathbb{Z}_{16}$.

23. $32 = 2^5$, giving

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_8 \times \mathbb{Z}_4, \quad \mathbb{Z}_{16} \times \mathbb{Z}_2, \quad \mathbb{Z}_{32}$.

24. $720 = 2^4 3^2 5$, giving $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, $\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

25. $1089 = 3^2 11^2$, giving $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$, $\mathbb{Z}_9 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{121}$, $\mathbb{Z}_9 \times \mathbb{Z}_{121}$.

26. $24 = 2^3 3$, giving “ $2 \times 2 \times 2 \times 3$, $4 \times 2 \times 3$, 8×3 ”;
$25 = 5^2$, giving “ 5×5, 25 ”;
so $24 \cdot 25$ has $2 \cdot 3 = 6$.

27. Each commutative group of order m is isomorphic (by Theorem 12) to $\prod_i \mathbb{Z}_{p_i^{r_i}}$, and each commutative group of order n to $\prod_i \mathbb{Z}_{p_i'^{r_i'}}$ for some p_i, p'_i, r_i, r'_i. Then $\prod_i \mathbb{Z}_{p_i^{r_i}} \times \prod_i \mathbb{Z}_{p_i'^{r_i'}}$ is a group of order mn. Since $p_i \neq p'_j$ there is no rearrangement of factors between the two ‘halves’ that gives the same order, so this product is unique for the given ‘halves’.
Conversely, any commutative group of order nm can be written (by Theorem 12, reordering factors as required) as $\prod_i \mathbb{Z}_{p_i^{r_i}} \times \prod_i \mathbb{Z}_{p_i'^{r_i'}}$.
Thus there are exactly $\left| \prod_i \mathbb{Z}_{p_i^{r_i}} \right| \cdot \left| \prod_i \mathbb{Z}_{p_i'^{r_i'}} \right| = rs$ groups.

28. $10^5 = (2 \cdot 5)^5 = 2^5 5^5$. By (23) there are 7 groups of order k^5, so there are 49.

29. a. For each order, the possible group factorings are:
2: 2, 11 (2)
3: 3, 21, 111 (3)
4: 4, 31, 22, 211, 1111 (5)
5: 5, 41, 32, 311, 221, 2111, 1111 (7)
6: 6, 51, 42, 411, 33, 321, 3111, 222, 2211, 21111, 111111 (11)
7: 7, 61, 52, 511, 43, 421, 4111, 331, 322, 3211, 31111, 2221 22111, 211111, 1111111 (15)
8: 8, 71, 62, 611, 53, 521, 5111, 44, 431, 422, 4211, 41111, 332, 3311, 3221, 32111, 311111, 2222, 22211, 221111, 21111111, 11111111 (22)
b. $3 \cdot 5 \cdot 15 = 225$; $15 \cdot 15 = 225$; $22 \cdot 5 = 110$.

30. a. true
b. true
c. false
d. true
e. false ($\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic whereas $\mathbb{Z}_8$ is)
f. false ($|S_8| = 8!$ whereas $\mathbb{Z}_2 \times \mathbb{Z}_4 = 8$)
g. false? (there is no element of S_4 of order 8 that generates the subgroup isomorphic to $\mathbb{Z}_8$)
h. false ($|\langle \varepsilon \rangle| = 1$)
i. true
j. true

31. $Z_2 = \{0, 1\}$.

32. a. 1, because every proper subgroup has fewer elements than the group.
b. ∞, because $\forall n \in \mathbb{N}^* : n\mathbb{Z} \cong \mathbb{Z}$.

33. $|S_3| = 3! = 6$.

34. a. true (Corollary 3.11)
b. false (the Klein 4-group V is not cyclic, and $|V| = 4 = 2^2$)
c. false ($1 \notin \langle \{4, 6\} \rangle = \langle 2 \rangle$)
d. true ($\langle \{4, 5, 6\} \rangle = \langle 1 \rangle = \mathbb{Z}_8$)

e. true

f. false ($\mathbb{Z}_2 \not\cong \mathbb{Z}_3$ both have Betti number 0)

g. true (by Theorem 16 $G \cong \mathbb{Z}_{5^i} \times \ldots$, and $\mathbb{Z}_{5^i}$ is cyclic)

h. false (it could be that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$; but there exist G for which it is true)

i. false (by Theorem 16, there is no isomorphic factorization containing $\mathbb{Z}_6$)

j. true

35. It is equal. For each commutative group of order p^r the factorization of Theorem 16 gives the structure of a corresponding group of order q^r.

36. $72 = 2^3 3^2$, so G must be isomorphic to one of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \ldots$, $\mathbb{Z}_8 \times \ldots$.

a. In each of the three cases, G has one subgroup of order 8.

b. In the first case, G has three subgroups of order 4; in the second case, two ($\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \subset \mathbb{Z}_4 \times \mathbb{Z}_2$); in the third case, one.

37. By Theorem 12, $G \cong \times_i \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}^m$. Then $H = \times_i \mathbb{Z}_{p_i^{r_i}} \times E^m$, since $\mathbb{Z}$ has no other elements of finite order, and $Z_{p_i^{r_i}}$ are finite so each of its elements are.

38. The torsion subgroup of $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$ is $\mathbb{Z}_4 \times E \times \mathbb{Z}_3$, which has $4 \cdot 3 = 12$ elements; that of $\mathbb{Z}_{12} \times Z \times \mathbb{Z}_{12}$ is $\mathbb{Z}_{12} \times E \times \mathbb{Z}_{12}$, which has $12 \cdot 12 = 144$ elements.

39. The only elements of finite order in $\mathbb{R}^*$ form its torsion subgroup $\left\langle \left\{ -1, +1 \right\} \right\rangle$.

40. The only elements of finite order in $\mathbb{C}^*$ form its torsion subgroup $\left\langle \left\{ 1, j, -1, -j \right\} \right\rangle$.

41. By Theorem 12, every finitely generated commutative group is isomorphic to $H = \times_i \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}^m$. $E \times \mathbb{Z}^n$ is obviously torsion-free, and $\times_i \mathbb{Z}_{p_i^{r_i}}$ is its torsion subgroup.

42. c. Let $G = \times_i \times_{j<n_i} \mathbb{Z}_{p_i^{q_{ij}}}$, $\forall i, j : q_{ij} \geq q_{i,j+1}$, then $T = \times_j \mathbb{Z}_{\cdot_{i:j<n_i} p_i^{q_{ij}}}$. For each prime p_i, q_{ij} are its powers in the factorization. Note that I reverse the order of the torsion coefficients because it simplifies the expressions.

a. $G = \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$, so $i = 0,1$; $n_0 = 1, n_1 = 1$; $p_0 = 2, p_1 = 3$; $q_{00} = 2, q_{10} = 2$. Then $T = \mathbb{Z}_{2^2 \cdot 3^2} = \mathbb{Z}_{36}$.

b. $G = \mathbb{Z}_{2^1 3^1} \times \mathbb{Z}_{2^2 3^1} \times \mathbb{Z}_{2^2 5^1}$, so $T = \mathbb{Z}_{2^2 \cdot 3^1 \cdot 5^1} \times \mathbb{Z}_{2^2 \cdot 3^1} \times \mathbb{Z}_{2^1} = \mathbb{Z}_{60} \times \mathbb{Z}_{12} \times \mathbb{Z}_2$ from
$i = 0,1,2$; $p_0 = 2, p_1 = 3, p_2 = 5$; $n_0 = 3, n_1 = 2, n_2 = 1$; $q_{00} = 2, q_{01} = 2, q_{02} = 1, q_{10} = 1, q_{11} = 1, q_{20} = 1$.

43. $\forall (g,h),(g',h') \in G \times H$: $(g,h) \cdot (g',h') = (g \cdot g', h \cdot h') = (g' \cdot g, h' \cdot h) = (g',h') \cdot (g,h)$, so $G \times H$ is commutative.

44. $H = \left\{ h \in G \mid \left| \left\langle h \right\rangle \right| = 2 \right\} \cup E \Rightarrow \quad \forall h \in H : \left\langle h \right\rangle = \left\{ e, h \right\}$.

- $e \in H$ (identity)
- $\forall h \in H : \left\langle h^{-1} \right\rangle = \left\langle h \right\rangle = \left\{ e, h \right\} \Rightarrow \quad \left| \left\langle h^{-1} \right\rangle \right| = 2 \Rightarrow \quad h^{-1} \in H$ (inverse)
- $\forall h, h' \in H \setminus E : hh' = h^{-1} \cdot h'^{-1} = h'^{-1} \cdot h^{-1} = (hh')^{-1} \Rightarrow \quad \left\langle hh' \right\rangle = \left\{ e, h \cdot h' \right\} \Rightarrow \quad \left| \left\langle hh' \right\rangle \right| = 2$ (closure)

so $H \subseteq G$.

45. a. $H = \left\{ h \in G \mid \left| \left\langle h \right\rangle \right| = 3 \right\} \cup E \Rightarrow \quad \forall h \in H : \left\langle h \right\rangle = \left\{ e, h, h^2 \right\}$.

- $e \in H$ (identity)
- $\forall h \in H : \left\langle h^{-1} \right\rangle = \left\langle h^2 \right\rangle = \left\{ e, h^2, h^4 \right\} = \left\{ e, h^2, h \right\} \Rightarrow \quad \left| \left\langle h^{-1} \right\rangle \right| = 3 \Rightarrow \quad h^{-1} \in H$ (inverse)
- $\forall h, h' \in H \setminus E : \begin{cases} h' \notin \left\langle h \right\rangle : & \left\langle hh' \right\rangle = \left\{ e, hh', (hh')^2 \right\} \\ h' = h : & \left\langle hh' \right\rangle = \left\langle h^2 \right\rangle = \left\langle h^{-1} \right\rangle \\ h' = h^2 : & hh' = e \end{cases} \Rightarrow \quad hh' \in H \cup E$ (closure).

so $H \subseteq G$.

b. $H = \left\{h \in G \mid \left|\langle h \rangle\right| = 4\right\} \cup E \Rightarrow \quad \forall h \in H : \langle h \rangle = \left\{e, h, h^2, h^3\right\}$. Then $\langle hh \rangle = \left\{e, h^2\right\} \Rightarrow \quad \left|\langle hh \rangle\right| \neq 4 \Rightarrow \quad H \not\subseteq G$.

c. For any n, the identity and inverse exist in the subgroup. Suppose n is divisible by m, then $\forall h \in H: \quad \left(h^m\right)^{n/m} = h^n = e \Rightarrow \quad \left|\langle h^m \rangle\right| = \frac{n}{m} < n \Rightarrow \quad h^m \notin H$, so n must be prime.

47. a. By Definition 1.

b. $$\left.\begin{aligned} hk &= (h,e) \times (e,k) = (he, ek) = (h,k) \\ kh &= (e,k) \times (h,e) = (eh, ke) = (h,k) \end{aligned}\right\} \Rightarrow \quad hk = kh.$$

c. $\forall h \in H,\ k \in K,\ h = k: \quad (h,e) = (e,k) \Rightarrow \quad h = e \wedge k = e \Rightarrow \quad H \cap K = E$.

48. $\forall h, h' \in H,\ k, k' \in K : hk = h'k' \Rightarrow \quad (h,e) \cdot (e,k) = (h',e) \cdot (e,k') \Rightarrow \quad (he, ek) = (h'e, ek') \Rightarrow \quad h = h' \wedge k = k'$. Also, $H \times K \cong H \times K$.

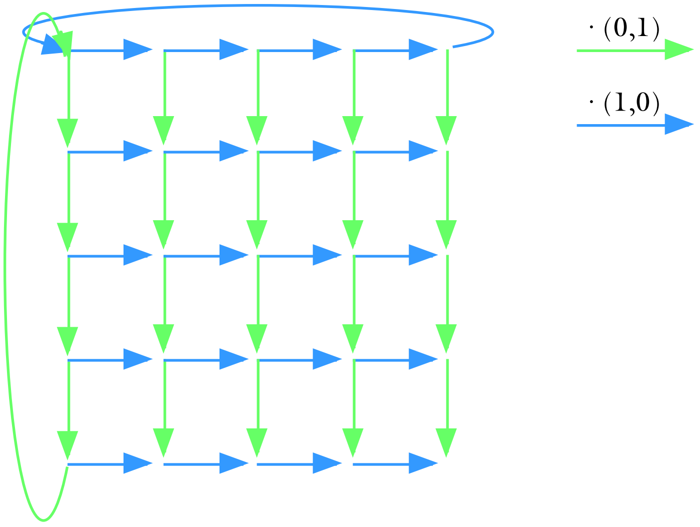
49. Consider the factorization of any finite commutative group by Theorem 12. If it contains a factor of the form $\mathbb{Z}_p \times \mathbb{Z}_p$, the group is not cyclic because that subgroup has no generator. Since the group is finite, it contains no $\mathbb{Z}$ factors. Any factors $\mathbb{Z}_p \times \mathbb{Z}_q$ where $p \neq q$ have (1,1) as generator, but factors $\mathbb{Z}_p \times \mathbb{Z}_{p^m} \supseteq \mathbb{Z}_p \times \mathbb{Z}_p$ have no generator.

50. By Theorem 12, any such group is isomorphic to $G = \prod_i \mathbb{Z}_{p_i^{r_i}}$. For each factor, $p_i^{r_i}$ is divisible only by a power of p, so the order of any element of $\mathbb{Z}_{p_i^{r_i}}$ is a power of p. So the order of any element of G is (Theorem 9) the least common multiple of powers of p, which is itself a power of p.
Is there a counterexample for noncommutative groups?

51. From the isomorphism,
$\exists \phi : G \times K \to H \times K : \forall (g,k),(g',k') \in G \times K : \phi\left((g,k)\right) \cdot \phi\left((g',k')\right) = \phi\left((g,k) \cdot (g',k')\right) = \phi\left((gg', kk')\right)$, so then
$\psi : G \to H : g \mapsto \phi_1(g,e)$ is an isomorphism between G and H.

52. It is easily verified that $\forall r < n-1 : (1\ 2\ 3 \ldots n)^{n-r}(1\ 2)(1\ 2\ 3 \ldots n)^r = (r+1 \quad r+2)$. Then $\forall a,b : a < b$, $(a\, b) = (a \quad a+1)(a+1 \quad a+2)\ldots(b-2 \quad b-1)(b-1 \quad b)(b-2 \quad b-1)\ldots(a+1 \quad a+2)(a \quad a+1)$. By Corollary 2.12, every $g \in S_n$ is a product of such transpositions, so the given set indeed generates S_n.

53.



54. a. G will be commutative when the inner and outer n-gons have the same orientation.

b. $\mathbb{Z}_2 \times \mathbb{Z}_n$.

c. If n is odd, $n = 2m+1: \quad \mathbb{Z}_2 \times \mathbb{Z}_n = \mathbb{Z}_2 \times \mathbb{Z}_{2m+1} \not\supseteq \mathbb{Z}_2 \times \mathbb{Z}_2$ it is (49) cyclic.

d. The dihedral group.

55. $fx = \sin 2\pi x$.

56. $fx = \sin \frac{2\pi}{\sqrt{3}} x$.

57. $f(x,y) = \sin 2\pi x \cdot \sin 2\pi y$.

58. $f(x,y) = \sin \frac{2\pi}{3} x \cdot \sin \frac{2}{\sqrt{5}} y$.

59. $f(x,y) = \sin 2x + \cos 3y = \sin \frac{2}{2\pi} 2\pi x + \cos \frac{3}{2\pi} 2\pi y$

$\tau_1(x,y) = \left(x + \frac{2\pi}{2}, y \right)$; $\tau_2(x,y) = \left(x, y + \frac{2\pi}{3} \right)$

60. $f(x,y) = \sin\left(12 \arctan \frac{y}{x} \right)$.

61. $f(x,y) = \sin\left(12 \arctan \frac{y+5}{x - \sqrt{3}} \right)$.

62. • the rotation over zero degrees is the identity isometry (identity)

• if $\mathrm{rot}_\alpha \in H \Rightarrow \quad \mathrm{rot}_\alpha^{-1} \in G \Rightarrow \quad \mathrm{rot}_\alpha^{-1} = \mathrm{rot}_{-\alpha} \in H$ (inverse)

• if $\mathrm{rot}_\alpha, \mathrm{rot}_\beta \in H \Rightarrow \quad \mathrm{rot}_\alpha \circ \mathrm{rot}_\beta \in G \Rightarrow \quad \mathrm{rot}_\alpha \circ \mathrm{rot}_\beta = \mathrm{rot}_{\alpha+\beta} \in H$ (closure)

so $H \subseteq G$. An isometry is either orientation-preserving or not, and isometry preservation is isomorphic to $\mathbb{Z}_2$ (e.g., the composition of a preserving with a non-preserving function is non-preserving, 0 + 1 = 1). The isometries in H are all the orientation-preserving ones. If there is at least one orientation non-preserving isometry in G, then $G \cong H \times \mathbb{Z}_2 \Rightarrow \quad |G| = 2|H|$. Otherwise, $G = H$.

63.

	rotation	h-reflection	v-reflection	glide	isomorphism
64.	N	N	N	N	Z
65.	N	N	Y	N	D_∞
66.	N	Y	N	N	$Z \times Z_2$
67.	Y	N	N	N	D_∞
68.	Y	Y	Y	N	$D_\infty \times Z_2$
69.	N	N	N	Y	Z
70.	Y	N	Y	Y	$Z \times D_\infty$?

71. a. $\theta \in \{0°, 90°, 180°, 270°\}$; b. yes; c. no. (see left figure)

72. a. $\theta \in \{0°, 180°\}$; b. yes; c. yes. (see center figure)

73. a. no; b. no; c. no.

74. a. no; b. yes; c. no.

75. a. $\theta \in \{0°, 180°\}$; b. yes; c. no.

76. a. $\theta \in \{0°, 120°, 240°\}$; b. yes; c. no. (see right figure)

77. a. $\theta \in \{0°, 120°, 240°\}$; b. yes; c. yes (? book says no).

78. a. no; b. no; c. yes; d. (1,0) and (0,1).

79. a. $\theta \in \{0°, 90°, 180°, 270°\}$; b. yes; c. no; d. (2,0) and (0,2) (why does the book say "(1,1)" and not just "(1,0)"?).

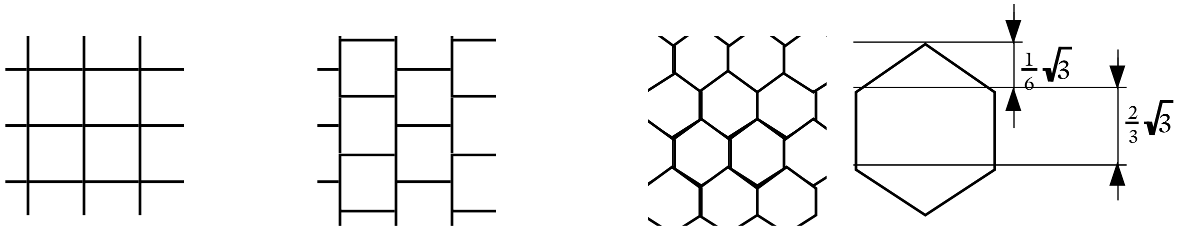
80. a. $\theta \in \{0°, 120°, 240°\}$; b. no; c. yes; d. (1,0) and (0,2)

81. a. $\theta \in \{0°, 120°, 240°\}$; b. yes; c. no; d. (0,1) and $(1, \sqrt{3})$.

82. Space rotation of a cube is a permutation of its four diagonal axes, so $G \subseteq S_4$. How many ways are there of permuting them? Fix one arbitrary axis— there are $2 \cdot 4 = 8$ ways of doing this. Then there remain three 120°

rotations along that axis, giving a total of $8 \cdot 3 = 24$ permutations. So $G = S_4$.

§2.5 Binary Linear Codes



1. 0B007F7F2500257F39 (hexadecimal).
2. “GONE_HOME”.
3. $x_4 = x_1 + x_2; \quad x_5 = x_1 + x_3; \quad x_6 = x_2 + x_3.$
4. 000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000.
5. An error in one bit generates an error in two parity bits; an error in two bits also generates an error in two parity bits; an error in three bits is never detected.
6. One- and two-bit errors both generate errors in two parity bits, so only one type can be reliably corrected.
7. $C + \{000111\} = \{000111, 001100, 010010, 011001, 100001, 101010, 110100, 111111\}.$
8. a. 110; b. 001; c. 110; d. 001, 100, 111; e. 101.
9. $$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$
10. a. $H \cdot [110111]^{\mathrm{T}} = [100]^{\mathrm{T}} \Rightarrow \quad 110.$

    b. $H \cdot [001011]^{\mathrm{T}} = [000]^{\mathrm{T}} \Rightarrow \quad 001.$

    c. $H \cdot [111011]^{\mathrm{T}} = [011]^{\mathrm{T}} \Rightarrow \quad 110.$

    d. $H \cdot [101010]^{\mathrm{T}} = [111]^{\mathrm{T}} \Rightarrow$ not decodable.

    e. $H \cdot [100101]^{\mathrm{T}} = [011]^{\mathrm{T}} \Rightarrow \quad 101.$

11.

000000	000
000001	001
000010	010
000100	100
001000	011
010000	101
100000	110

Hw	corrected	code
100	110011	110
000	001011	001
011	110011	110
111	incorrigible	
011	101101	101

12. a. $\mathrm{wt}(u) = 7$; b. $\mathrm{wt}(v) = 6$; c. $u + v = 1010011001$; d. 5.
13. $\forall v \in \mathbb{B}^n : v^{-1} \in \mathbb{B}^n : v + v^{-1} = 0 \Rightarrow \quad \forall i : v^{-1}{}_i = v_i \Rightarrow \quad v^{-1} = v$, so $u - v = u + v^{-1} = u + v$.
14. Because it has a “1” bit in each position where a transmission error occurred.

15. Because $u - v$ has a "1" bit in each position where u differs from v.

16. a. $\mathrm{d}(u, v) = 0 \Leftrightarrow$ u and v agree in each bit position $\Leftrightarrow u = v$.

b. In every bit position where u differs from v, v differs from u.

c. If u differs from w in some bit position, then u differs from v or w differs from v in that position, so $\mathrm{d}(u, v) + \mathrm{d}(w, v) \geq \mathrm{d}(u, w)$.

d. If $u_i = v_i$ for some bit position i, then also $u_i + 0 = v_i + 0, \quad u_i + 1 = v_i + 1$, so $u + w = v + w$.

17. $\mathbb{B}^n = \left(\mathbb{Z}_2\right)^n$.

18.
- $0000000 = e \in \mathbb{B}^n; \quad 0000000 \in C \Rightarrow e \in C$ (identity)
- $\forall x \in C: \overline{x} = \left(\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4\overline{x}_5\overline{x}_6\overline{x}_7\right)$ (inverse)

$$= \left(\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4\right)\left(\overline{x_1 + x_2 + x_3}\right)\left(\overline{x_1 + x_2 + x_3}\right)\left(\overline{x_1 + x_2 + x_3}\right)$$

$$= \left(\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4\right)\left(\overline{x}_1 + \overline{x}_2 + \overline{x}_3\right)\left(\overline{x}_1 + \overline{x}_3 + \overline{x}_4\right)\left(\overline{x}_2 + \overline{x}_3 + \overline{x}_4\right) \in C$$

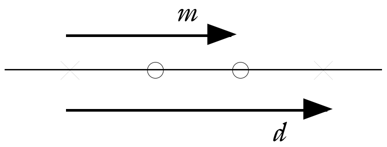
- $\forall x, y \in C: x + y =$

$$\begin{aligned}
&\left(x_1x_2x_3x_4x_5x_6x_7\right) + \left(y_1y_2y_3y_4y_5y_6y_7\right) = \\
&\left(x_1 + y_1 \quad x_2 + y_2 \quad x_3 + y_3 \quad x_4 + y_4 \quad x_5 + y_5 \quad x_6 + y_6 \quad x_7 + y_7\right) = \\
&\left(x_1 + y_1 \quad x_2 + y_2 \quad x_3 + y_3 \quad x_4 + y_4\right. \\
&\quad (x_1 + x_2 + x_3) + (y_1 + y_2 + y_3) \\
&\quad (x_1 + x_3 + x_4) + (y_1 + y_3 + y_4) \\
&\quad \left.(x_2 + x_3 + x_4) + (y_2 + y_3 + y_4)\right) = \\
&\left(x_1 + y_1 \quad x_2 + y_2 \quad x_3 + y_3 \quad x_4 + y_4\right. \\
&\quad (x_1 + y_1) + (x_2 + y_2) + (x_3 + y_3) \\
&\quad (x_1 + y_1) + (x_3 + y_3) + (x_4 + y_4) \\
&\quad \left.(x_2 + y_2) + (x_3 + y_3) + (x_4 + y_4)\right) = \\
&\left((x + y)_1 \quad (x + y)_2 \quad (x + y)_3 \quad (x + y)_4 \quad (x + y)_5 \quad (x + y)_6 \quad (x + y)_7\right) \in C
\end{aligned}$$

so $C \subseteq \mathbb{B}^7$.

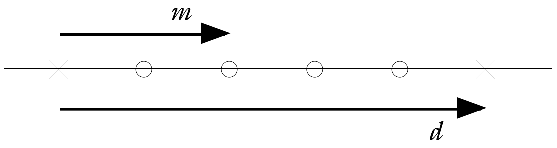
19. $\forall c, d \in C : c \neq d : \mathrm{d}(c, d) \overset{16d}{=} \mathrm{d}(c - d, d - d) = \mathrm{d}(c - d, 0) \overset{15}{=} \mathrm{wt}\left((c - d) - 0\right) = \mathrm{wt}(c - d)$, where $c - d$ is some element of C.

20.



$d = m + 1$

21.



$d = 2m + 1$

22. From Exercise 19, the minimum nonzero weight of code words is the minimum distance between code words. Then we can detect $2t + 1 = m + 1 \Rightarrow \quad m = 2t$ and correct $2t + 1 = 2m + 1 \Rightarrow \quad m = t$ errors.

23. For there to be a minimum distance of 3 between code words, changing one bit in each of two code words may map those two code words into the same coset. The number of cosets is thus the number of ways of changing 0 or 1 bits in a code word, so $2^{n-k} \geq 1 + n$.

24. Similarly, the number of cosets is the number of ways of changing 0, 1, or 2 bits in a code word, so $2^{n-k} \geq 1 + n + \frac{1}{2}n(n - 1)$.

25. Simply try the formula with increasing value of n:

k	m	$n-k$
a. 2	3	3
b. 4	3	3
c. 8	3	4
d. 2	5	5
e. 4	5	6
f. 8	5	7

26. $$G=\begin{bmatrix}1&&&&&1&1&&\\&1&&&&1&&1&\\&&1&&&1&&&1\\&&&1&&&1&1&\\&&&&1&&1&&1\end{bmatrix}$$. By Exercise 24, $n-k\geq 4$.

27. $$G=\begin{bmatrix}1&&&&&&&&1&1&&\\&1&&&&&&&1&&&1\\&&1&&&&&&1&&1&\\&&&1&&&&&1&&1&1\\&&&&1&&&&1&1&1&\\&&&&&1&&&&1&&1\\&&&&&&1&&&1&1&\\&&&&&&&1&&1&&1\end{bmatrix}$$. By Exercise 24, $n-k\geq 4$.

28. a. $\mathrm{wt}(0)=0 \Rightarrow \quad 0\in H$ (identity). $\forall h\in H: h^{-1} \overset{13}{=} h \Rightarrow \quad \mathrm{wt}(h^{-1})=\mathrm{wt}(h) \Rightarrow \quad x^{-1}\in H$ (inverse). Finally, see that $\mathrm{wt}(x+y)=\mathrm{wt}(x)+\mathrm{wt}(y)-2a$, where a is the number of positions where $x_i=y_i=1$ (closure).

b. A word is either even or odd. Let $x\in G$ be odd, then $\forall h\in H: xh$ is odd, and because G is a group, xH is a coset of G so $G=H\cup xH$.

29.

3.1 Homomorphisms

1. $\forall a,b\in\mathbb{Z}:\phi(a+_{\mathbb{Z}}b)=\phi a+_{\mathbb{Z}}\phi b$.

2. $\phi\left(\frac{1}{2}+_{\mathbb{R}}\frac{1}{2}\right)=\phi 1=1,\quad \phi\frac{1}{2}+\mathbb{Z}\phi\frac{1}{2}=0+_{\mathbb{Z}}0=0$.

3. $\forall a,b\in\mathbb{R}^{*}:\phi(ab)=|ab|=|a|\cdot|b|=\phi a\cdot\phi b$.

4. $\forall a,b\in\mathbb{Z}_6: a=2a_2+a_0,\ b=2b_2+b_0$.

$$\phi\left(a+_{\mathbb{Z}_6}b\right)=\phi\left(2\left(a_2+b_2\right)+_{\mathbb{Z}_6}\left(a_0+b_0\right)\right)=\left(a_0+b_0\right)\operatorname{mod}2=$$
$$a_0+_{\mathbb{Z}_2}b_0=\phi\left(2a_2+a_0\right)+_{\mathbb{Z}_2}\phi\left(2b_2+b_0\right)=\phi a+_{\mathbb{Z}_2}\phi b$$

5. $\phi\left(8+_{\mathbb{Z}_9}1\right)=\phi 0=0;\quad \phi 8+_{\mathbb{Z}_2}\phi 1=0+_{\mathbb{Z}_2}1=1$. ϕ is an 'even-odd' calculator, but in $\mathbb{Z}_9$, 8 and 8 + 1 are both even.

6. $\forall a,b\in\mathbb{R}:\phi(a+_{\mathbb{Z}}b)=2^{a+b}=2^{a}\cdot 2^{b}=\phi a\cdot\phi b$.

7. $\forall g_i,g_i'\in G_i:\phi_i\left(g_i\cdot g_i'\right)=\left(e_1,\ldots,g_i\cdot g_i',\ldots,e_r\right)\overset{\text{def.}}{=}\left(e_1,\ldots,g_i,\ldots,e_r\right)\cdot\left(e_1,\ldots,g_i',\ldots,e_r\right)=\phi_i g_i\cdot\phi_i g_i'$.

8. If G is commutative, $\forall g,g'\in G:\quad \phi\left(gg'\right)=\left(gg'\right)^{-1}=g'^{-1}g^{-1}=g^{-1}g'^{-1}=\phi g\cdot\phi g'$. If G is not commutative, f is not generally an isomorphism.

9. $\forall f,g\in F:\phi(f+g)=\dfrac{\mathrm{d}^2(f+g)}{\mathrm{d}x^2}=\dfrac{\mathrm{d}^2 f}{\mathrm{d}x^2}+\dfrac{\mathrm{d}^2 g}{\mathrm{d}x^2}=\phi f+\phi g$.

10. $\forall f,g\in F:\phi(f+g)=\int_0^4 f+g\,\mathrm{d}x=\int_0^4 f\,\mathrm{d}x+\int_0^4 g\,\mathrm{d}x=\phi f\cdot\phi g$.

11. $\forall f,g \in F : \phi(f+g) = 3(f+g) = 3f + 3g = \phi f + \phi g$.

12. $\phi\left(\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}+\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right)=\phi\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}=\begin{vmatrix}1 & 0\\0 & 1\end{vmatrix}=1;\quad \phi\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}+\phi\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}=\begin{vmatrix}1 & 0\\0 & 0\end{vmatrix}+\begin{vmatrix}0 & 0\\0 & 1\end{vmatrix}=0+0=0$.

13. $\forall \mathbf{A},\mathbf{B} \in M_n : \phi(\mathbf{A}+\mathbf{B}) = \mathrm{tr}(\mathbf{A}+\mathbf{B}) = \sum_i a_i + b_i = \sum_i a_i + \sum_i b_i = \mathrm{tr}\mathbf{A} + \mathrm{tr}\mathbf{B}$.

14. Since $\mathrm{GL}(n,\mathrm{R}) \subseteq M_n$, the proof of Exercise 13 holds.

15. $f(x) = x \Rightarrow \quad \phi(f+f) = \int_0^1 (f\cdot f)(x)\,\mathrm{d}x = \int_0^1 x^2\,\mathrm{d}x = \frac{1}{3}x^3$

$$\phi(f) = \int_0^1 f(x)\,\mathrm{d}x = \int_0^1 x\,\mathrm{d}x = \tfrac{1}{2}x^2 \Rightarrow \quad \phi(f)+\phi(f) = x^2$$

16. $\mathrm{Ker}\,\phi = A_3$.

17. $\phi_4 : \mathbb{Z} \to \mathbb{Z} : n \mapsto 4n$ is a homomorphism by Example 7, and $\gamma_7 : \mathbb{Z} \to \mathbb{Z}_7 : n \mapsto n \bmod 7$ is by Example 10, so $\phi = \gamma_7 \circ \phi_4$, $\quad \phi 1 = 4\cdot 1 \bmod 7 = 4 \bmod 7 = 4$ is a homomorphism. Then
$\mathrm{Ker}\,\phi = \mathrm{Ker}\,\gamma_7 \circ \phi_4 = (\gamma_7 \circ \phi_4)^{\mathrm{inv}} 0 = \phi_4^{\mathrm{inv}} 7\mathbb{Z} = \frac{7}{4}\mathbb{Z} \cap \mathbb{Z} = 7\mathbb{Z};\quad \phi 25 = (\gamma_7 \circ \phi_4) 25 = \gamma_7 100 = 2$.

18. Let $\phi = \gamma_{10} \circ \phi_6;\quad \phi 1 = 6$. Then
$\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}} 0 = (\gamma_{10} \circ \phi_6)^{\mathrm{inv}} 0 = \phi_6^{\mathrm{inv}} 10\mathbb{Z} = \frac{10}{6}\mathbb{Z} \cap \mathbb{Z} = \frac{5}{3}\mathbb{Z} \cap \mathbb{Z} = 5\mathbb{Z};\quad \phi 18 = (\gamma_{10} \circ \phi_6) 18 = \gamma_{10} 108 = 8$.

19. First, note that $(1\ 4\ 2\ 6)(2\ 5\ 7) = (1\ 4\ 2\ 5\ 7\ 6)$. Let $\phi : \mathbb{Z} \to S_8 : n \mapsto (1\ 4\ 2\ 5\ 7\ 6)^n$, then
$\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}}() = 6\mathbb{Z};\quad \phi 20 = (1\ 4\ 2\ 5\ 7\ 6)^{\ 2} = (1\ 2\ 7)(4\ 5\ 6)$.

20. Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20} : n \mapsto 8 \cdot_{\mathbb{Z}_{20}} n;\quad \phi 1 = 8$, then $\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}} 0 = \frac{20}{8}\mathbb{Z} \cap \mathbb{Z}_{10} = 10\mathbb{Z} + 5;\quad \phi 3 = 8 \cdot_{\mathbb{Z}_{20}} 3 = 4$.

21. Let $\phi : \mathbb{Z}_{24} \to S_8 : n \mapsto ((2\ 5)(1\ 4\ 6\ 7))^n;\quad \phi 1 = (2\ 5)(1\ 4\ 6\ 7)$, then
$\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}} 0 = 4\mathbb{Z} \cap \mathbb{Z}_{24} = \{0,4,8,12,16,20\};\quad \phi 14 = ((2\ 5)(1\ 4\ 6\ 7))^2 = (1\ 6)(4\ 7)$.

22. Let $\phi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z} : (x,y) \mapsto 3x - 5y;\quad \phi(1,0) = (2,-3), \phi(0,1) = (-1,5)$, then
$\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}} 0 = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} \mid 3x - 5y = 0\};\quad \phi(-3,2) = 3\cdot -3 - 5\cdot 2 = -9 - 10 = -19$.

23. Let $\phi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z} : (x,y) \mapsto (2x - y, -3x + 5y);\quad \phi(1,0) = (2,-3), \phi(0,1) = (-1,5)$, then
$\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}} 0 = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} \mid 2x - y = 0 \wedge -3x + 5y = 0\} = \{(0,0)\}$, because
$\begin{cases}2x - y = 0\\ -3x + 5y = 0\end{cases} \Rightarrow \begin{cases}y = 2x\\ -3x + 10x = 7x = 0\end{cases} \Rightarrow \begin{cases}y = 0\\ x = 0\end{cases}$, and $\phi(4,6) = (2\cdot 4 - 6, -3\cdot 4 + 5\cdot 6) = (2,18)$.

24. $\phi : \mathbb{Z}\times\mathbb{Z} \to S_{10} : (x,y) \mapsto ((3\ 5)(2\ 4))^x((1\ 7)(6\ 10\ 8\ 9))^y;\quad \phi(1,0) = (3\ 5)(2\ 4), \phi(0,1) = (1\ 7)(6\ 10\ 8\ 9)$,
then $\mathrm{Ker}\,\phi = \phi^{\mathrm{inv}} 0 = 2\mathbb{Z}\times 4\mathbb{Z};\quad \phi(3,10) = ((3\ 5)(2\ 4))^1((1\ 7)(6\ 10\ 8\ 9))^2 = (3\ 5)(2\ 4)(6\ 8)(10\ 9)$.

25. There are two: $\phi_1 : \mathbb{Z} \to \mathbb{Z} : i \mapsto i;\quad \phi_{-1} : \mathbb{Z} \to \mathbb{Z} : i \mapsto -i$.

26. $\forall n \in \mathrm{N} :\quad \phi_n : \mathbb{Z} \to \mathbb{Z} : m \mapsto nm$.

27. There are two: $\phi_1 : \mathbb{Z} \to \mathbb{Z}_2 : i \mapsto i \bmod 2;\quad \phi_0 : \mathbb{Z} \to \mathbb{Z}_2 : i \mapsto 0$.

28. $\forall x,y \in G : \phi_g(xy) = \phi_g x \cdot \phi_g y \Rightarrow \quad g(xy) = gx \cdot gy \Rightarrow \quad xy = xgy \Rightarrow \quad y = gy \Rightarrow \quad g = e$.

29. $\forall x,y \in G : \phi_g(xy) = \phi_g x \cdot \phi_g y \Rightarrow \quad g(xy)g^{-1} = gxg^{-1} \cdot gyg^{-1} = gxyg^{-1} \Rightarrow \quad g \in G$.

30. A group homomorphism of a group G into a group G' is a map $\phi : G \to G'$ such that for all $x,y \in G$ …

31. OK

32. a. true (odd times even equals even times odd)
b. true (the trivial homomorphism)
c. false (the trivial homomorphism)
d. true (Corollary 18)
e. false (there are 4 cosets in G, but 4 does not divide 6)
f. false (ϕ is a function, so $|\phi G| \le |G|$)

g. true (the trivial homomorphism)
h. true (the trivial homomorphism)
i. false ($\phi e \cdot \phi e = \phi e \Rightarrow \quad \phi e = e \Rightarrow \quad e \in \operatorname{Ker}\phi$)
j. false ($\phi : \mathbb{Z}_2 \to \mathbb{Z} \times \mathbb{Z}_2 : i \mapsto (0,i)$)

33. No, there must be 5 cosets in G, but 5 does not divide 12.

34. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4 : i \mapsto i \bmod 4$.

35. $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_5 : (i,j) \mapsto (i,0)$.

36. No.

37. $\phi : \mathbb{Z}_3 \to S_3 : i \mapsto \begin{pmatrix}1 & 2 & 3\end{pmatrix}^i$.

38. $\phi : \mathbb{Z} \to S_3 : i \mapsto \begin{pmatrix}1 & 2 & 3\end{pmatrix}^i$.

39. $\phi : \mathbb{Z} \times \mathbb{Z} \to 2\mathbb{Z} : (x,y) \mapsto 2x$.

40. $\phi : 2\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} : i \mapsto (i,0)$.

41. $\phi : D_4 \to S_3 : \begin{cases} \rho_0, \rho_1, \rho_2, \rho_3 \mapsto (1\ \ 2)^0 \\ \mu_1, \mu_2, \delta_1, \delta_2 \mapsto (1\ \ 2)^1 \end{cases}$.

42. $\phi : S_3 \to S_4 : s \mapsto s$.

43. $\phi : S_4 \to S_3 : \begin{cases} s \text{ even } \mapsto (1\ \ 2)^0 \\ s \text{ odd } \mapsto (1\ \ 2)^1 \end{cases}$.

44. ϕ partitions G into $|\phi G|$ cosets (Theorem 15), so $|\phi G|$ divides $|G|$. Also, since ϕ is a function $|\phi G| < |G| \Rightarrow \quad |G| < \infty \Rightarrow |\phi G| < \infty$.

45. $\phi G \subseteq G' \Rightarrow \quad |\phi G| < |G'| < \infty$. Also, $\phi G \subseteq G' \Rightarrow \quad |\phi G|$ divides $|G'|$.

46. $\forall g \in G : g = \cdot_i a_{k_i} \Rightarrow \quad \phi g = \phi \cdot_i a_{k_i} = \cdot_i \phi a_{k_i} = \cdot_i \mu a_{k_i} = \mu \cdot_i a_{k_i} = \mu g \Rightarrow \quad \phi = \mu$.

47. By Exercise 44, $|\phi G|$ divides $|G|$, so $|\phi G| = 1$ (trivial homomorphism) $\vee\, |\phi G| = |G|$ (injective map) .

48. Obvious. $\operatorname{Ker}\phi = A_n$.

49. $\forall g, g' \in G : \gamma\phi(gg') = \gamma(\phi g \cdot \phi g') = \gamma\phi g \cdot \gamma\phi g'$.

50. ϕG commutative $\quad \Leftrightarrow \quad \forall h, h' \in \phi G \subseteq H : hh' = h'h \quad \Leftrightarrow \quad h = h'hh'^{-1} \quad \Leftrightarrow \quad h'hh'^{-1}h^{-1} = e$.

$$\Leftrightarrow \quad \forall g, g' \in G : \phi\left(g'gg'^{-1}g^{-1}\right) \overset{\text{Theorem 12.2}}{=} \phi g' \cdot \phi g \cdot (\phi g')^{-1} \cdot (\phi g)^{-1} = e$$

$$\Leftrightarrow \quad \forall g, g' \in G : g'gg'^{-1}g^{-1} \in \operatorname{Ker}\phi$$

51. $\forall n, m \in \mathbb{Z} : \phi(nm) = a^{nm} = a^n a^m = \phi n \cdot \phi m$. $\phi\mathbb{Z} = \langle a \rangle, \quad \operatorname{Ker}\phi = \mathbb{Z}_{|\langle a \rangle|}$ (where $\mathbb{Z}_\infty \equiv E$).

52.

53. $\forall m, n \in \mathbb{Z} \times \mathbb{Z} : \phi(mn) = \phi m \cdot \phi n \Leftrightarrow$.

$$\phi((m_1, m_2) \cdot (n_1, n_2)) = \phi((m_1, m_2)) \cdot \phi((n_1, n_2)) \Leftrightarrow$$

$$\phi(m_1 n_1, m_2 n_2) = \phi(m_1, m_2) \cdot \phi(n_1, n_2) \Leftrightarrow$$

$$h^{m_1 n_1} k^{m_2 n_2} = h^{m_1} k^{m_2} h^{n_1} k^{n_2} \Leftrightarrow$$

$$kh = hk, \text{ so } \langle\{h, k\}\rangle \text{ is commutative}$$

54. $\forall h, k \in G : hk = kh \quad \Leftrightarrow \quad G$ is commutative.

55. $\forall i, j \in \mathbb{Z}_n : \phi(ij) = \phi i \cdot \phi j \quad \Leftrightarrow \quad h^{i +_{\mathbb{Z}_n} j} = h^i h^j \Leftarrow \begin{cases} h = e \\ |\langle h \rangle| = n \end{cases} \Leftrightarrow \quad h^n = e$.

3.2 Factor Groups

1. $\left|\mathbb{Z}_6/\langle 3\rangle\right| = \left|\mathbb{Z}_6\right|/\left|\langle 3\rangle\right| = 6/2 = 3$.

2. $\left|\mathbb{Z}_4 \times \mathbb{Z}_{12}/\langle 2\rangle \times \langle 2\rangle\right| = \left|\mathbb{Z}_4/\langle 2\rangle\right| \cdot \left|\mathbb{Z}_{12}/\langle 2\rangle\right| = 2 \cdot 2 = 4$.

3. $\left|\mathbb{Z}_4 \times \mathbb{Z}_2/\langle (2,1)\rangle\right| = 8/2 = 4$.

4. $\left|\mathbb{Z}_3 \times \mathbb{Z}_5/\{0\} \times \mathbb{Z}_5\right| = \left|\mathbb{Z}_3/\{0\}\right| \cdot \left|\mathbb{Z}_5/\mathbb{Z}_5\right| = 3 \cdot 1 = 3$.

5. $\left|\mathbb{Z}_2 \times \mathbb{Z}_4/\langle (1,1)\rangle\right| = \left|\mathbb{Z}_2 \times \mathbb{Z}_4\right|/\left|\langle (1,1)\rangle\right| = 8/4 = 2$.

6. $\left|\mathbb{Z}_{12} \times \mathbb{Z}_{18}/\langle (4,3)\rangle\right| = \left|\mathbb{Z}_{12} \times \mathbb{Z}_{18}\right|/\left|\langle (4,3)\rangle\right| = 216/6 = 36$.

7. $\left|\mathbb{Z}_2 \times S_3/\langle (1,\rho_1)\rangle\right| = \left|\mathbb{Z}_2 \times S_3\right|/\left|\langle (1,\rho_1)\rangle\right| = 12/6 = 2$.

8. $\left|\mathbb{Z}_{11} \times \mathbb{Z}_{15}/\langle (1,1)\rangle\right| = \left|\mathbb{Z}_{11} \times \mathbb{Z}_{15}\right|/\left|\langle (1,1)\rangle\right| = 161/161 = 1$.

9. $\left|5 + \langle 4\rangle\right|_{\mathbb{Z}_{12}/\langle 4\rangle} = \left|1 + \langle 4\rangle\right|_{\mathbb{Z}_{12}/\langle 4\rangle} = \left|\{1,2,3,4 = 0\} + \langle 4\rangle\right| = 4$.

10. $\left|26 + \langle 12\rangle\right|_{\mathbb{Z}_{60}/\langle 12\rangle} = \left|2 + \langle 12\rangle\right|_{\mathbb{Z}_{60}/\langle 12\rangle} = \left|\{2,4,6,8,10,12 = 0\} + \langle 12\rangle\right| = 6$.

11. $\left|(2,1) + \langle (1,1)\rangle\right|_{\mathbb{Z}_3 \times \mathbb{Z}_6/\langle (1,1)\rangle} = \left|(1,0) + \langle (1,1)\rangle\right|_{\mathbb{Z}_3 \times \mathbb{Z}_6/\langle (1,1)\rangle} = \left|\{(1,0),(2,0),(3 = 0,0)\} + \langle (1,1)\rangle\right| = 3.$

12. $\left|(3,1) + \langle (1,1)\rangle\right|_{\mathbb{Z}_4 \times \mathbb{Z}_4/\langle (1,1)\rangle} = \left|(2,0) + \langle (1,1)\rangle\right|_{\mathbb{Z}_4 \times \mathbb{Z}_4/\langle (1,1)\rangle} = \left|\{(2,0),(4 = 0,0)\} + \langle (1,1)\rangle\right| = 2$.

13. $\left|(3,1) + \langle (0,2)\rangle\right|_{\mathbb{Z}_4 \times \mathbb{Z}_8/\langle (0,2)\rangle} = \left|\{(3,1),(6 = 2,2 = 0),(5 = 1,1),(4 = 0,2 = 0)\} + \langle (0,2)\rangle\right| = 4$.

14. $\left|(3,3) + \langle (1,2)\rangle\right|_{\mathbb{Z}_4 \times \mathbb{Z}_8/\langle (1,2)\rangle} = \left|(4 = 0,5) + \langle (1,2)\rangle\right|_{\mathbb{Z}_4 \times \mathbb{Z}_8/\langle (1,2)\rangle} = \left|\{(0,5),(0,10 = 2 = 0)\} + \langle (1,2)\rangle\right| = 2$.

15. $\left|(2,0) + \langle (4,4)\rangle\right|_{\mathbb{Z}_6 \times \mathbb{Z}_8/\langle (4,4)\rangle} = \left|(-2 = 4,-4 = 4) + \langle (4,4)\rangle\right|_{\mathbb{Z}_6 \times \mathbb{Z}_8/\langle (4,4)\rangle} = \left|(0,0) + \langle (4,4)\rangle\right|_{\mathbb{Z}_6 \times \mathbb{Z}_8/\langle (4,4)\rangle} = 1$.

16. $i_{\rho_1} : S_3 \to S_3 : \sigma \mapsto \rho_1 \sigma \rho_1^{-1} : i_{\rho_1}\{\rho_0, \mu_1\} = \left\{\rho_1 \rho_0 \rho_1^{-1} = \rho_0,\ \rho_1 \mu_1 \rho_1^{-1} = \mu_2\right\}$.

17. Replace "for all $h \in H$" with "for all $g \in G$".

18. The book definition says "$ghg^{-1} \in H$", but this definition is equivalent.

19. Replace "into" with "onto". This makes the homomorphism an isomorphism, which is what an automorphism is supposed to be.

20. A normal subgroup can be used to form a factor group.

21. a. This doesn't necessarily have to be nonsense, but apparently students that write $a \in G/H$ don't realize that $a = g_a H,\ g_a \in G$. Since they don't realize that elements of G/H are sets (cosets of H), the proofs make no sense.
    b. "Let aH and bH be two elements of G/H."
    c. $\forall aH, bH \in G/H : (aH)(bH) = a(Hb)H \overset{H\text{ normal}}{=} a(bH)H \overset{G\text{ commutative}}{=} (ba)HH \overset{H\text{ normal}}{=} b(Ha)H = (bH)(aH)$.

22. a. See Exercise 21a.
    b. See Exercise 21b.
    c. $\forall gH \in G/H : \exists n \in \mathrm{N} : g^n = e \Rightarrow (gH)^n \overset{\text{Theorem 4}}{=} g^n H = eH = H$, which is the identity element of G/H.

23. a. true (if N is not normal, the factor group does not exist— Definition 6)
    b. true (Example 8)
    c. true ($i_g : G \to G : x \mapsto gxg^{-1} \overset{\text{commutative}}{=} xgg^{-1} = x$)
    d. true (G cannot have more cosets than elements)
    e. true (Exercise 22)
    f. false ($\left|\mathbb{Z}/2\mathbb{Z}\right| = 2$)
    g. true (Exercise 21)
    h. false (G/G is commutative)
    i. true (Example 7)

j. false ($n\mathbb{R} = \mathbb{R} \Rightarrow \quad \mathbb{R}/n\mathbb{R} = E$)

24. All permutations of A are even, and those of $S\backslash A$ are all odd. $\{A, S\setminus A\}$ are the cosets of A in S. If $\sigma \in S_n$ is even, so are $\sigma A = A\sigma$; similarly if σ is odd.

	$\sigma_{\text{even}}A$	$\sigma_{\text{even}}A$
$\sigma_{\text{even}}A$	$\sigma_{\text{even}}A$	$\sigma_{\text{odd}}A$
$\sigma_{\text{odd}}A$	$\sigma_{\text{odd}}A$	$\sigma_{\text{even}}A$

$\Leftrightarrow$

$\mathbb{Z}_2$	0	1
0	0	1
1	1	0

The group is isomorphic to $\mathbb{Z}_2$.

25.

26. G is commutative, so the subgroup T is normal in G.

$\exists gT \in G/T : \exists n \in N^* : (gT)^n = T \Rightarrow \quad g^n T = T \Rightarrow \quad g^n \in T$, so G/T is indeed torsion-free.

27.
- $\forall H \subseteq G: \quad i_e(H) = H$ (reflexive)
- $\forall H, K \subseteq G : H \sim K \Rightarrow \quad \exists g \in G : i_g H = K \Rightarrow \quad \forall k \in K : \exists h \in H : i_g h = k \Rightarrow$ (symmetric)

  $i_{g^{-1}} k = i_{g^{-1}} i_g h = i_{g^{-1}}\left(ghg^{-1}\right) = \left(g^{-1}\right)\left(ghg^{-1}\right)\left(g^{-1}\right)^{-1} = h \Rightarrow \quad i_{g^{-1}} K = H \Rightarrow \quad K \sim H$
- $\forall H, K, L \subseteq H: \quad H \sim K, K \sim L \Rightarrow \quad \exists g, g' \in G : K = i_g H, L = i_{g'} K \Rightarrow$ (transitive)

  $\forall h \in H : i_{g'g} h = (g'g)h(g'g)^{-1} = g'ghg^{-1}g'^{-1} = g'\left(ghg^{-1}\right)g'^{-1} = g'\left(i_g h\right)g'^{-1} = i_{g'} i_g h = i_{g'} i_g h \Rightarrow$

  $i_{g'g} H = L \Rightarrow \quad H \sim L$

28. If H is normal to G, then by the discussion after Definition 9, the image of H under all the inner automorphisms is H itself. So H is normal iff its cell of the partition under conjugacy contains only itself.

29. $\left\{i_{\rho_2} = i_{\mu_3}, \quad i_{\rho_0} = i_{\mu_2}, \quad i_{\rho_1} = i_{\mu_1}\right\} = \left\{\{\rho_0, \mu_1\}, \{\rho_0, \mu_2\}, \{\rho_0, \mu_3\}\right\}$.

30.

31. Let $H, K \subseteq G$ be normal. $\forall g \in G: \quad g(H \cap K) \subseteq Hg \wedge g(H \cap K) \subseteq Kg \Rightarrow \quad g(H \cap K) \subseteq Hg \cap Kg = (H \cap K)g$. From the converse, $g(H \cap K) = (H \cap K)g$.

32. Suppose there were two distinct 'smallest' normal subgroups containing S, then their intersection would be smaller, contain S, and be (Exercise 31) normal.

33.

34. If G has one subgroup H of order $|H|$, then H must be invariant under all inner automorphisms, so (by the discussion after Definition 9) H is normal.

35. $H \cap N \subseteq H$ by Exercise 1.5.54. $\forall h \in H: \quad h(H \cap K) \in H \cap K \Rightarrow \quad h(H \cap K) = H \cap K$, and by the converse, $(H \cap K)k = H \cap K$, so $h(H \cap K) = (H \cap K)h$.

36.

37. a. $\forall g \in G : i_e \circ i_g : \forall x \in G : \left(i_e \circ i_g\right)x = i_e i_g x = i_g x \Rightarrow \quad i_e \circ i_g = i_e$ (identity)

$\forall g \in G : i_{g^{-1}} \circ i_g : \forall x \in G : \left(i_{g^{-1}} \circ i_g\right)x = i_{g^{-1}}\left(gxg^{-1}\right) = g^{-1}\left(gxg^{-1}\right)g = x \Rightarrow \quad i_{g^{-1}} \circ i_g = i_e$ (inverse)

$\forall g, h, k \in G : \left(i_g \circ i_h\right) \circ i_k = i_g \circ \left(i_h \circ i_k\right)$ because function composition is associative (associative)

b.

38.

39. Let $\phi^* : G/H \to G'/H' : gH \mapsto (\phi g)H'$. This is a homomorphism if $\forall gH, g'H \in G/H$,

$\phi^*(gH \cdot g'H) = \phi^* gH \cdot \phi^* g'H \Leftarrow \quad \phi^*((gg')H) = \phi^* gH \cdot \phi^* g'H \Leftarrow$

$\phi(gg')H' = (\phi g \cdot H') \cdot (\phi g' \cdot H') = (\phi g \cdot \phi g') \cdot H' \Leftarrow \quad \phi(gg') = \phi g \cdot \phi g'$

which holds because ϕ is an isomorphism.

40. a. $H = \{M \in \mathrm{GL}(n, \mathrm{R}) \mid \det M = 1\}$ is normal in G because

$\forall g \in G, h \in H : ghg^{-1} \in H \Leftarrow \quad \det ghg^{-1} = \det g \cdot \det h \cdot \det g^{-1} = \det g \cdot \det h \cdot (\det g)^{-1} = \det h = 1$.

b. $H = \{M \in \mathrm{GL}(n, \mathrm{R}) \mid \det M = \pm 1\}$ is normal in G because of a similar argument.

41. a. $\forall A,B,C \subseteq G:\quad (AB)C = \{ab \mid a \in A, b \in B\}C = \{(ab)c \mid a \in A, b \in B, c \in C\} = \{a(bc) \mid \ldots\} = A\{bc \mid \ldots\} = A(BC)$ (associativity). $E \subseteq G \Rightarrow \quad \forall H \subseteq G : EH = \{eh \mid e \in E, h \in H\} = \{h \mid h \in H\} = H$ (identity). Suppose G has an inverse G' in its power set, then $GG' = E \Rightarrow \quad \{gg' \mid g \in G, g' \in G'\} = \{e\}$, but $\left|\{gg' \mid \ldots\}\right| \geq |G| \geq |E|$.

b.

c. Let $M = \{m \subseteq G \mid m \text{ is a coset of } N\} = \{gN \mid g \in G\}$. The operation is associative, as shown in (a). $\forall gN \in M: (gN)N = \{g\}NN = \{g\}N \in N$, so N is an identity in M. Finally, because N is normal in G, $\forall gN \in M: \left(g^{-1}N\right) \cdot (gN) = \left(\{g^{-1}\}N\right) \cdot (\{g\}N) = \{g^{-1}\}N\{g\}N = \left(\{g^{-1}\}\{g\}\right)NN = \{e\}N = N$ (inverse).

§3.3 Factor-Group Computations and Simple Groups

1. $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(0,1)\rangle \cong \mathbb{Z}_2 \times \{0\} \cong \mathbb{Z}_2$.
2. $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(0,2)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
3. $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(1,2)\rangle \cong \mathbb{Z}_4$.
4. $\mathbb{Z}_4 \times \mathbb{Z}_8 / \langle(1,2)\rangle \cong \mathbb{Z}_8$.
5. $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8 / \langle(1,2,4)\rangle = \mathbb{Z}_4 \times \mathbb{Z}_8$.
6. $\mathbb{Z} \times \mathbb{Z} / \langle(0,1)\rangle = \mathbb{Z}$.
7. $\mathbb{Z} \times \mathbb{Z} / \langle(1,2)\rangle = \mathbb{Z}$.
8. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} / \langle(1,1,1)\rangle = \mathbb{Z} \times \mathbb{Z}$.
9. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_4 / \langle(3,0,0)\rangle = \mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}_4$.
10. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 / \langle(0,4,0)\rangle = \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8$.
11. $\mathbb{Z} \times \mathbb{Z} / \langle(2,2)\rangle = \mathbb{Z}_2 \times \mathbb{Z}$.
12. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} / \langle(3,3,3)\rangle = \mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}$.
13. $\mathrm{Z}\, D_4 = \{\rho_0, \rho_2\}$. Is the center a natural choice for a minimal normal subgroup? In any case, $D_4 / Z = \{\rho_0 Z, \rho_1 Z, \mu_1 Z, \delta_1 Z\}$ is commutative, by manual verification, so by Theorem 20 $Z \subseteq C$. But $D_4 / E \cong D_4$ is not commutative, so $E \not\subseteq C \Rightarrow \quad C = Z$.
14. First, note that for any commutative group $\forall a,b \in G : aba^{-1}b^{-1} = ab(ba)^{-1} = (ab)(ab)^{-1} = e$, so $\mathrm{C}\,G = E$. Then, $\mathrm{Z}\,\mathbb{Z}_3 = \mathbb{Z}_3$, and by Example 19 $\mathrm{Z}\,S_3 = E$. Further, $\mathrm{C}\,\mathbb{Z}_3 = E$, and by Example 21 $\mathrm{C}\,S_3 = A_3$. So $\mathrm{Z}(\mathbb{Z}_3 \times S_3) = \mathbb{Z}_3 \times E, \quad \mathrm{C}(\mathbb{Z}_3 \times S_3) = E \times A_3$.
15. $\mathrm{Z}(S_3 \times D_4) = \mathrm{Z}\,S_3 \times \mathrm{Z}\,D_4 =$ (Example 19, Exercise 13) $E \times \{\rho_0, \rho_2\}$
$\mathrm{C}(S_3 \times D_4) = \mathrm{C}\,S_3 \times \mathrm{C}\,D_4 =$ (Example 21, Exercise 13) $A_3 \times \{\rho_0, \rho_2\}$
16. Subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_4$ with one generator (cyclic):

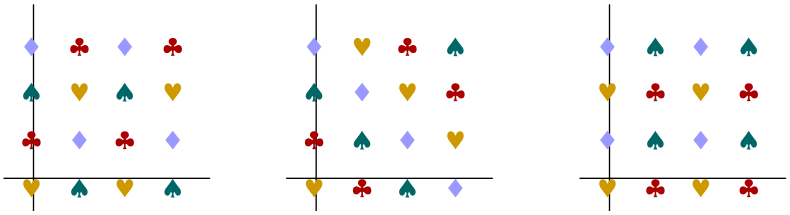
<...>	{<...>}	|...|	$\mathbb{Z}_4 \times \mathbb{Z}_4 / < \ldots >$
(0,0)	(0,0)	1	$\mathbb{Z}_4 \times \mathbb{Z}_4$
(0,1)	(0,0) (0,1) (0,2) (0,3)	4	$\mathbb{Z}_4 \times \mathbb{Z}_1$
(0,2)	(0,0) (0,2)	2	$\mathbb{Z}_4 \times \mathbb{Z}_2$
(0,3) ~ (0,1)			
(1,0)	(0,0) (1,0) (2,0) (3,0)	4	$\mathbb{Z}_1 \times \mathbb{Z}_4$
(1,1)	(0,0) (1,1) (2,2) (3,3)	4	$\mathbb{Z}_4$
(1,2)	(0,0) (1,2) (2,0) (3,2)	4	$\mathbb{Z}_4$ (figure left)
(1,3)	(0,0) (1,3) (2,2) (3,1)	4	$\mathbb{Z}_4$ (figure center)

(2,0)	(0,0) (2,0)	2	$\mathbb{Z}_2 \times \mathbb{Z}_4$
(2,1)	(0,0) (2,1) (0,2) (2,3)	4	$\mathbb{Z}_4$
(2,2)	(0,0) (2,2)	2	$\mathbb{Z}_2 \times \mathbb{Z}_4$

(2,3) ~ (2,1)
$(3,n) \sim (1,n)$
Subgroups with two generators (not cyclic), with order less than or equal to 4:

(0,2) (2,0)	(0,0) (0,2) (2,0) (2,2)	4	V (figure right)

(0,2) (2,2) ~ (0,2) (2,0)
(2,0) (2,2) ~ (2,0) (0,2)
There are no subgroups with more than two generators with order less than or equal to 4.



17. “The center of a group G *is a set containing* all…”

18. The book uses “ $aba^{-1}b^{-1}$”, but this definition is equivalent.

19. a. true (Theorem 9)
b. false (by Exercise 16, $G/G \cong E$)
c. false ($\left.\frac{1}{2}\right|_{\mathbb{R}/\mathbb{Z}} + \left.\frac{1}{2}\right|_{\mathbb{R}/\mathbb{Z}} = 0_{\mathbb{R}/\mathbb{Z}}$)
d. true ($\left.\frac{1}{n}\right|_{\mathbb{R}/\mathbb{Z}}$)
e. false ($\left.1\frac{1}{2}\right|_{\mathbb{R}/\mathbb{Z}} = \left.\frac{1}{2}\right|_{\mathbb{R}/\mathbb{Z}}$).
f. true (Exercise 14)
g. false (not $C \subseteq H$ but $H \subseteq C$)
h. false (when G is simple and commutative)
i. true (By Theorem 20, the commutator subgroup is normal to G, so if G is simple then C is trivial or nonproper. But if C were trivial, then $G/E \cong G$ would be commutative. So C is nonproper.)
j. false (by Theorem 15, A_5 is nontrivial, finite, simple, and of 5! nonprime order)

20. $\{f \in F \mid f\,0 = 0\} \subseteq F$.

21. $\{f \in F^* \mid f\,0 = 1\} \subseteq F^*$.

22. The cosets each represent a specific additive discontinuity, of the form $a \cdot \theta(x-b)$, where θ is the step function. An element of order two would represent a discontinuity that is its own inverse, which under addition could only be the identity discontinuity, which has order one.

23. See Exercise 22. Each discontinuity with $a < 0$ is its own inverse under multiplication, and has order two.

24. $z_0 U = U \Rightarrow \quad U/z_0 U \cong E$.

25. $\langle -1 \rangle_U = \{-1,+1\}; \quad U/\langle -1 \rangle \cong U$.

26. $\langle z_n \rangle \cong \mathbb{Q}; \quad U/\langle z_n \rangle \cong U$.

27. $\mathbb{R}/\mathbb{Z} \cong [0,1[\cong U$.

28. $\mathbb{Z}$ has $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

29. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_4$, then $\mathbb{Z}_1 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_1$ but $\mathbb{Z}_2 \times \mathbb{Z}_4 / \mathbb{Z}_2 \times \mathbb{Z}_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \not\cong \quad \mathbb{Z}_2 \times \mathbb{Z}_4 / \mathbb{Z}_2 \times \mathbb{Z}_1 = \mathbb{Z}_1 \times \mathbb{Z}_4$.

30. a. The center of every commutative group consists of all the elements of that same group.
b. Suppose $\exists z \in Z\,G : \forall g \in G : zg = gz \Rightarrow \quad \forall z^n \in \langle z \rangle, n \in \mathbb{N} : z^n g = g z^n$, so $\langle z \rangle$ is normal to G and, since G is simple, wither trivial or nonproper. Since $\langle z \rangle$ is commutative but G is not, $\langle z \rangle \cong E$, so $Z = E$.

31. a. If G is commutative, then $G \cong G/E$ is too, so by Theorem 20 $C \subseteq E \Rightarrow \quad C = E$.

b. Since G is not commutative, by the same argument $C \not\subseteq E \Rightarrow \quad C \neq E$. Since G is simple, C must then be nonproper.

simple group G	not commutative	commutative
center $\mathrm{Z}G$	E	G
commutator $\mathrm{C}G$	G	E

32. If $H \subseteq G$ such that G/H exists, then H is normal to G. Since $G : H > 1 \Rightarrow \quad H \subset G$, and since H is nontrivial $H \supset E$. So H is a proper nontrivial normal subgroup of G, so G is not simple.

33. $\forall g' \in G' : g' \cdot \phi N = \phi N \cdot g' \Leftarrow \quad \phi\phi^{\text{inv}} g' \cdot \phi N = \phi N \cdot \phi\phi^{\text{inv}} g' \Leftarrow \quad \phi\left(\phi^{\text{inv}} g' \cdot N\right) = \phi\left(N \cdot \phi^{\text{inv}} g'\right) \Leftarrow$

$$\phi^{\text{inv}} g' \cdot N = N \cdot \phi^{\text{inv}} g' \Leftarrow \quad \forall g \in \phi^{\text{inv}} g' : gN = Ng \Leftarrow \quad N \text{ is normal.}$$

34.

35. Suppose $G/\mathrm{Z}G$ is cyclic, then $\exists g^* \,\mathrm{Z}G \in G/\mathrm{Z}G : \left\langle g^* \,\mathrm{Z}G \right\rangle = G/\mathrm{Z}G$, and

$\forall g \in G : \exists n \in \mathbb{N} : g \in \left(g^* \,\mathrm{Z}G\right)^n = g^{*n} \,\mathrm{Z}G \Rightarrow \quad \exists z \in \mathrm{Z}G : g = g^{*n} z$. Then

$$\forall g, g' \in G : \exists z, z' \in \mathrm{Z}G, n, n' \in \mathbb{N} : gg' = \left(g^{*n} z\right)\left(g^{*n'} z'\right) = zg^{*n} g^{*n'} z' = z\left(g^*\right)^{n+n'} z' = zg^{*n} g^{*n'} z' =$$

$$g^{*n'} zz'g^{*n} = g^{*n'} z'zg^{*n} = \left(g^{*n'} z'\right)\left(g^{*n} z\right) = g'g$$

so G is commutative. So if G is not commutative, $G/\mathrm{Z}G$ is not cyclic.

36. Since $|G| = pq$, the order of any subgroup of G must (Lagrange) have order pq, p, q, or 1, and the resultant factor group must therefore have order 1, q, p, or pq. By Exercise 35, the factor group $G/\mathrm{Z}G$ is not cyclic. Since all groups of prime order are cyclic, the factor group must have order pq, so $|\mathrm{Z}G| = 1 \Rightarrow \quad \mathrm{Z}G = E$.

37. a. $(i\ j\ k) = (i\ j)(j\ k)$, so every 3-cycle is the even product of transpositions and is therefore in A_n. Obviously A_n only contains 3-cycles if $n \geq 3$.

b. A_n consists of all products of even transpositions. Every type of even transposition

$(a\ b)(a\ b) = (a\ b\ c)^0; \quad (a\,b)(a\ d) = (a\ d\,b); \quad (a\,b)(c\ d) = (a\,c\ b)(a\ c\ d)$

can be formed from 3-cycles, A_n is generated by the 3-cycles.

c. For any r, s: $(r\ s\,i)^2(r\ s\ k)(r\ s\ j)^2(r\ s\,i) = (r\ i\ s)(r\ s\ k)(r\ j\ s)(r\ s\ i) = (i\ j\ k)$, so $\{_i(r\ s\ i)\}$ generates every 3-cycle in A_n and therefore A_n itself.

d. Let N be normal to A_n and $\exists(r\ s\,i) \in N$, then $\forall j : ((r\ s)(i\ j))(r\ s\ i)^2((r\ s)(i\ j))^{-1} = (r\ s\,j) \in N$, so $\{_i(r\ s\ i)\} \subseteq N \Rightarrow \quad N = A_n$.

e. First, 'canonicalize' the elements of N into products of disjoint cycles. Then, one of the following cases must hold:

1• N contains a 3-cycle, so by (d.) $N = A_n$.

2• N contains a product in which at least one of the cycles has length greater than 3, $\sigma = \mu(a_1\ a_2\ a_3 \ldots a_r)$. Then

$\sigma^{-1}(a_1\ a_2\ a_3)\sigma(a_1\ a_2\ a_3)^{-1} \overset{\sigma \in N}{=} (h \in N)\,\sigma^{-1}h \overset{\sigma^{-1} \in N}{\in}$ N, and

$$\sigma^{-1}(a_1\ a_2\ a_3)\sigma(a_1\ a_2\ a_3)^{-1} = \left(\mu(a_1\ a_2\ a_3 \ldots a_r)\right)^{-1}(a_1\ a_2\ a_3)\sigma(a_1\ a_2\ a_3)^{-1} =$$

$$(a_1\ a_2\ a_3 \ldots\ a_r)^{-1}\mu^{-1}(a_1\ a_2\ a_3)\mu(a_1\ a_2\ a_3 \ldots a_r)(a_1\ a_2\ a_3)^{-1} \overset{\text{disjoint}}{=}$$

$$(a_1\ a_2\ a_3 \ldots a_r)^{-1}(a_1\ a_2\ a_3)(a_1\ a_2\ a_3 \ldots a_r)(a_1\ a_2\ a_3)^{-1} =$$

$$(a_1\ a_3\ a_r)(a_2)({}_{3<k<r}\ a_k) = (a_1\ a_3\ a_r)$$

so Case 1• applied.

3• N contains no single 3-cycle or products with cycles of length greater than 3, but contains a product of at least two 3-cycles, $\sigma = \mu(a_1\ a_2\ a_3)(a_4\ a_5\ a_6)$. Then

$\sigma^{-1}(a_1\ a_2\ a_4)\sigma(a_1\ a_2\ a_4)^{-1} \overset{\sigma \in N}{=} (h \in N)\,\sigma^{-1}h \overset{\sigma^{-1} \in N}{\in}$ N, and

$$\sigma^{-1}(a_1\ a_2\ a_4)\sigma(a_1\ a_2\ a_4)^{-1} \overset{\text{disjoint}}{=} (a_4\ a_5\ a_6)^{-1}(a_1\ a_2\ a_3)^{-1}(a_1\ a_2\ a_4)(a_1\ a_2\ a_3)(a_4\ a_5\ a_6)(a_1\ a_2\ a_4)^{-1} = (a_1\ a_4\ a_2\ a_3\ a_6)(a_5)$$

so Case 2• applied.

4• N contains no products with cycles of length greater than 3, no products with more than one 3-cycle, and no 3-cycles, but contains a product with one 3-cycle, $\sigma = \mu(a_1\ a_2\ a_3)$, where μ is an even product of 2-cycles. Then

$\sigma^2 \overset{\sigma\in N}{\in} N$, and $\sigma^2 \overset{\text{disjoint}}{=} \mu^2(a_1\ a_2\ a_3)^2 \overset{\substack{\mu\text{ are}\\ \text{transpositions}}}{=} (a_1\ a_2\ a_3)^2 = (a_1\ a_3\ a_2)$, so Case •1 applied.

5• N contains no products containing cycles of length greater than or equal to 3. Since N is nontrivial and consists solely of products of even transpositions, it must contain an element $\sigma = \mu(a_1\ a_2)(a_3\ a_4)$. Then

$\sigma^{-1}(a_1\ a_2\ a_3)\sigma(a_1\ a_2\ a_3)^{-1} \overset{\sigma\in N}{=} (h \in N)\ \sigma^{-1}h \overset{\sigma^{-1}\in N}{\in} N$, and

$\sigma^{-1}(a_1\ a_2\ a_3)\sigma(a_1\ a_2\ a_3)^{-1} \overset{\text{disjoint}}{=} (a_3\ a_4)^{-1}(a_1\ a_2)^{-1}(a_1\ a_2\ a_3)(a_1\ a_2)(a_3\ a_4)(a_1\ a_2\ a_3)^{-1} = (a_1\ a_3)(a_2\ a_4)$.

Call this product α. Since $n \geq 5$, there is an a_5, and let $\beta = (a_3\ a_1\ a_5)$. Then

$\beta^{-1}\alpha\beta\alpha = (\beta^{-1})\alpha(\beta^{-1})^{-1}\alpha \overset{\alpha\in N}{=} (\gamma \in N)\ \gamma\alpha \in N$, and

$\beta^{-1}\alpha\beta\alpha = (a_3\ a_1\ a_5)^{-1}(a_1\ a_3)(a_2\ a_4)(a_3\ a_1\ a_5)(a_1\ a_3)(a_2\ a_4) = (a_1\ a_5\ a_3)(a_2)(a_4) = (a_1\ a_5\ a_3)$,

so Case 1• applied.

So, Case 1• always applies, so $N = A_5$.

38. • (closure) $\forall hn, h'n' \in HN : (hn)(h'n') = hnh'n' \overset{N\text{ normal}}{=} (n'' \in N, h'' \in H)\ hnn''h'' = h(nn'')h'' = (n''' \in N, h''' \in H)\ hh'''n''' = (hh''')n''' \in HN$

• (identity) $\forall hn \in HN : (ee)(hn) = eehn = ehn = hn$.

• (inverse) $\forall hn \in HN : (hn)^{-1}(hn) = n^{-1}h^{-1}hn = n^{-1}n = e$.

So $HN \subseteq G$. A subgroup containing both N and H must contain at least $\langle N \cup H\rangle = \langle\{_i\ n_i\} \cup \{_i\ h_i\}\rangle \supseteq \langle\{_{ij}\ n_i h_j\}\rangle = HN$, so HN must be the smallest subgroup that does.

39. M is normal to $G \Rightarrow\ M \subseteq G \Rightarrow\ NM \subseteq G$. Then

$\forall nm \in NM, g \in G : g(nm)g^{-1} = gng^{-1}gmg^{-1} \overset{N, M\text{ normal}}{=} (n' \in N, m' \in M)\ n'm' \in NM$, so NM is normal in G.

40. $$\forall h \in H, k \in K : hkh^{-1}k^{-1} = \begin{cases} (hkh^{-1})k^{-1} \overset{K\text{ normal}}{=} (k' \in K)\ k'k^{-1} \in K \\ h(kh^{-1}k^{-1}) \overset{H\text{ normal}}{=} (h' \in H)\ hh' \in H \end{cases} = e\text{, so } C = E,$$

so $E \subseteq C \Rightarrow\ \langle H \cup K\rangle / E \cong \langle H \cup K\rangle$ is commutative.

§3.4 Series of Groups

1. The two series

$\{0\} \subset 10\mathbb{Z} \subset \mathbb{Z}\quad (\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z},\ \ 10\mathbb{Z}/\{0\} \cong \mathbb{Z}_{10})$

$\{0\} \subset 25\mathbb{Z} \subset \mathbb{Z}\quad (\mathbb{Z}/25\mathbb{Z} \cong \mathbb{Z},\ \ 25\mathbb{Z}/\{0\} \cong \mathbb{Z}_{25})$

have isomorphic refinements

$\{0\} \subset 250\mathbb{Z} \subset 10\mathbb{Z} \subset \mathbb{Z}$

$\{0\} \subset 250\mathbb{Z} \subset 25\mathbb{Z} \subset \mathbb{Z}$

2. The two series

$\{0\} \subset 60\mathbb{Z} \subset 20\mathbb{Z} \subset \mathbb{Z}\quad (\mathbb{Z}, \mathbb{Z}_3, \mathbb{Z}_{20})$

$\{0\} \subset 245\mathbb{Z} \subset 49\mathbb{Z} \subset \mathbb{Z}\quad (\mathbb{Z}, \mathbb{Z}_5, \mathbb{Z}_{49})$

have isomorphic refinements

$\{0\} \subset 14700\,\mathbb{Z} \subset 300\,\mathbb{Z} \subset 60\mathbb{Z} \subset 20\mathbb{Z} \subset \mathbb{Z}$

$\{0\} \subset 14700\,\mathbb{Z} \subset 735\,\mathbb{Z} \subset 245\mathbb{Z} \subset 49\mathbb{Z} \subset \mathbb{Z}$

3. The two series

$\{0\} \subset \langle 3\rangle \subset \mathbb{Z}_{24} \quad (\mathbb{Z}_8, \mathbb{Z}_3)$

$\{0\} \subset \langle 8\rangle \subset \mathbb{Z}_{24} \quad (\mathbb{Z}_3, \mathbb{Z}_8)$

are already isomorphic.

4. The two series

$\{0\} \subset \langle 18\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{72} \quad (\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_3)$

$\{0\} \subset \langle 24\rangle \subset \langle 12\rangle \subset \mathbb{Z}_{72} \quad (\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_{12})$

have isomorphic refinements

$\{0\} \subset \langle 36\rangle \subset \langle 18\rangle \subset \langle 9\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{72}$

$\{0\} \subset \langle 24\rangle \subset \langle 12\rangle \subset \langle 6\rangle \subset \langle 2\rangle \subset \mathbb{Z}_{72}$

5. The two series

$\{(0,0)\} \subset 60\mathbb{Z} \times \mathbb{Z} \subset 10\mathbb{Z} \times \mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z} \quad (\mathbb{Z} \times \mathbb{Z}, \mathbb{Z}_6 \times E, \mathbb{Z}_{10} \times E)$

$\{(0,0)\} \subset \mathbb{Z} \times 80\mathbb{Z} \subset \mathbb{Z} \times 20\mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z} \quad (\mathbb{Z} \times \mathbb{Z}, E \times \mathbb{Z}_4, E \times \mathbb{Z}_{20})$

have isomorphic refinements

$\{(0,0)\} \subset 60\mathbb{Z} \times 80\mathbb{Z} \subset 60\mathbb{Z} \times 20\mathbb{Z} \subset 60\mathbb{Z} \times \mathbb{Z} \subset 10\mathbb{Z} \times \mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z}$

$\{(0,0)\} \subset 60\mathbb{Z} \times 80\mathbb{Z} \subset 10\mathbb{Z} \times 80\mathbb{Z} \subset \mathbb{Z} \times 80\mathbb{Z} \subset \mathbb{Z} \times 20\mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z}$

(this is not the answer the book gives, but seems okay)

6. Because $60 = 2 \cdot 2 \cdot 3 \cdot 5$, the composition series are of the form

$\mathbb{Z}_{60} \supset \langle 2\rangle_{\mathbb{Z}_{60}} \supset \langle 2 \cdot 2 = 4\rangle_{\mathbb{Z}_{60}} \supset \langle 2 \cdot 2 \cdot 3 = 12\rangle_{\mathbb{Z}_{60}} \supset \langle 2 \cdot 2 \cdot 3 \cdot 5 = 60\rangle_{\mathbb{Z}_{60}} = E$

where the series of generators are formed from the following 12 permutations of the factorization of 60:

2 2 3 5
2 2 5 3
2 3 2 5
2 3 5 2
2 5 2 3
2 5 3 2
3 2 2 5
3 2 5 2
3 5 2 2
5 2 2 3
5 2 3 2
5 3 2 2

The series that are thus constructed are obviously isomorphic.

7. As in Exercise 6, the series of generators are formed from the following 5 permutations of the factorization of $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$:

2 2 2 2 3
2 2 2 3 2
2 2 3 2 2
2 3 2 2 2
3 2 2 2 2

8. $\mathbb{Z}_5 \times \mathbb{Z}_3 \supset E \times \mathbb{Z}_3 \supset E \times E = E$

$\mathbb{Z}_5 \times \mathbb{Z}_3 \supset \mathbb{Z}_5 \times E \supset E \times E = E$

9. $S_3 \times \mathbb{Z}_2 \supset A_3 \times \mathbb{Z}_2 \supset E \times \mathbb{Z}_2 \supset E \times E = E$

$S_3 \times \mathbb{Z}_2 \supset S_3 \times E \supset A_3 \times E \supset E \times E = E$

Isn't the following a composition series too?

$S_3 \times \mathbb{Z}_2 \supset A_3 \times \mathbb{Z}_2 \supset A_3 \times E \supset E \times E = E$

10. $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset E \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset E \times E \times \mathbb{Z}_7 \subset E \times E \times E = E$
$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset E \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset E \times \mathbb{Z}_5 \times E \subset E \times E \times E = E$
$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset \mathbb{Z}_2 \times E \times \mathbb{Z}_7 \subset E \times E \times \mathbb{Z}_7 \subset E \times E \times E = E$
$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset \mathbb{Z}_2 \times E \times \mathbb{Z}_7 \subset \mathbb{Z}_2 \times E \times E \subset E \times E \times E = E$
$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset \mathbb{Z}_2 \times \mathbb{Z}_5 \times E \subset E \times \mathbb{Z}_5 \times E \subset E \times E \times E = E$
$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \subset \mathbb{Z}_2 \times \mathbb{Z}_5 \times E \subset \mathbb{Z}_2 \times E \times E \subset E \times E \times E = E$

11. $\mathrm{Z}(S_3 \times \mathbb{Z}_4) = \mathrm{Z}\,S_3 \times \mathrm{Z}\,\mathbb{Z}_4 = E \times \mathbb{Z}_4$.

12. $\mathrm{Z}(S_3 \times D_4) = \mathrm{Z}\,S_3 \times \mathrm{Z}\,D_4 = E \times \{\rho_0, \rho_2\}$.

13. $E \times E, E \times \mathbb{Z}_4, \ldots$.

14. $E \times E, E \times \{\rho_0, \rho_2\}, E \times D_4, \ldots$
Since $D_4 / \{\rho_0, \rho_2\}$ is of order four, it is commutative, so $\mathrm{Z}(D_4/\{\rho_0, \rho_2\}) = D_4/\{\rho_0, \rho_2\}$ which maps to D_4 under the canonical homomorphism.

15. Okay.

16. "A solvable group is one that has a composition series of which the factor groups are all commutative."

17. a. true ($G_i \lhd G \Rightarrow \quad G_i \lhd G_{i+1}$)
b. false ($G_i \lhd G_{i+1} \not\Rightarrow \quad G_i \lhd G$)
c. true
d. false
e. false ($E \subset \langle 3 \rangle_{\mathbb{Z}_{15}} \subset \mathbb{Z}_{15}$ and $E \subset \langle 5 \rangle_{\mathbb{Z}_{15}} \subset \mathbb{Z}_{15}$)
f. true ($E \subset G$ can be finitely refined)
g. false (S_7 is not solvable (h.), but $E \subset A_7 \subset S_7$ is a composition series with simple factor groups)
h. false ($E \subset A_7 \subset S_7$ is a composition series, but A_7 is not commutative)
i. true
j. true (Every finite group of prime order is cyclic and thus commutative. Every finite group has a composition series, and each of the factor groups is commutative because each of the numerator groups is a commutative subgroup of a commutative group.)

18. $S_3 \times S_3 \supset A_3 \times A_3 \supset E \times E; \quad S_3 \times S_3 / A_3 \times A_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2, \quad A_3 \times A_3 / E \times E \cong A_3 \times A_3$
is solvable because it has a composition series with commutative factors.

19. $D_4 \supset \{\rho_0, \rho_2\} \supset E; \quad |D_4 / \{\rho_0, \rho_2\}| = 4, \quad |\{\rho_0, \rho_2\}/E| = 2$
is solvable because it has a composition series with commutative factors.

20. $|H_{i+1}| = |H_{i+1}/H_i| \cdot |H_i| \Leftarrow \quad |H_{i+1}/H_i| = |H_{i+1}| / |H_i|$

$$|H_k| = \frac{|H_k|}{|H_0|} = \cdot_i \left| \frac{H_{i+1}}{H_i} \right| = s_1 \cdot \ldots \cdot s_k$$

21. Suppose $\subset_i H_i$ is such a composition series. Then $\exists k$: $|H_k| < \infty, |H_{k+1}| = \infty$. But then H_{k+1}/H_k is commutative with infinite order, so by the Exercise it has a proper normal subgroup and is this not simple.

22. Concatenate the factor groups' composition series into a series for the product group:
$E \cong \times_i E \quad \subset_{k \geq 0} \subset_{i > 1} \left(\times_{j<k} H_{j,n_j} \times H_{k,i} \times_{j>k} H_{j,0} \right) \quad \subset \times_i H_{i,n_i}$

§3.5 Group Action on a Set

♥ It is simplest to think of a G-set as a group of functions, where the group operations is just function composition. The functions operate as permutations on some set.

1.

$g \in G$	X_g
$\rho_0 = e$	X
ρ_1	$\{C\}$
ρ_2	$\{m_1, m_2, d_1, d_2, C\}$
ρ_3	$\{C\}$
μ_1	$\{s_1, s_3, m_1, m_2, C, P_1, P_3\}$
μ_2	$\{s_2, s_4, m_1, m_2, C, P_2, P_4\}$
δ_1	$\{2, 4, d_1, d_2, C\}$
δ_2	$\{1, 3, d_1, d_2, C\}$

2.

$x \in X$	G_x
1,3	$\{\rho_0, \delta_2\}$
2,4	$\{\rho_0, \delta_1\}$
s_1, s_3	$\{\rho_0, \mu_1\}$
s_2, s_4	$\{\rho_0, \mu_2\}$
m_1, m_2	$\{\rho_0, \rho_2, \mu_1, \mu_2\}$
d_1, d_2	$\{\rho_0, \rho_2, \delta_1, \delta_2\}$
C	D_4
P_1, P_3	$\{\rho_0, \mu_1\}$
P_2, P_4	$\{\rho_0, \mu_2\}$

3. $\{1,2,3,4\}$, $\{s_1, s_2, s_3, s_4\}$, $\{m_1, m_2\}$, $\{d_1, d_2\}$, $\{C\}$, $\{P_1, P_2, P_3, P_4\}$.

4. Insert “ $\forall x \in X$”.

5. Insert “ $\forall x \in X$” and delete “other”.

6. The G-set can be thought of as a direct product of its orbits. A sub-G-set consists of a subset of the orbits of the G-set.

7. A G-set is transitive iff it has exactly one orbit.

8. a. false (the elements of a G-set are not associative)
   b. true (Definition 1, Condition 1)
   c. false (G may not ‘act faithfully’)
   d. true (g are permutations, which are injective)
   e. false (any number of distinct permutations may operate on any particular element in the same way)
   f. true (Exercise 7)
   g. true ($H \subseteq G$ automatically abides by the same Conditions of Definition 1)
   h. true (they are the same orbits, but not necessarily *all* of them)
   i. true (Example 2)
   j. true (G consists of $|Gx|$ cosets of $|G_x|$ elements, each coset of which permutes x in a different way in its orbit)

9. a. $\phi : \{s_1, s_2, s_3, s_4\} \to \{P_1, P_2, P_3, P_4\} : s_i \mapsto P_i$.
   b. $\delta_2 \in G$ leaves 1 and 3 fixed in their orbit, but leaves no elements of the orbit $\{s_1, s_2, s_3, s_4\}$ fixed.
   c. $\{m_1, m_2\}$ and $\{d_1, d_2\}$ are not isomorphic. But trivially, any direct product of the two isomorphic sets of (a.) with any other orbit, is again isomorphic.

10. a. Yes, there is only $e \in G$ that leaves all the elemens of X fixed.
    b. $\{1,2,3,4\}$, $\{s_1, s_2, s_3, s_4\}$, $\{P_1, P_2, P_3, P_4\}$.

11.

12. • (identity) $\exists e \in G : \forall x \in X : ex = x \Rightarrow \quad \forall y \in \Upsilon \subseteq X : ey = y \Rightarrow \quad G_\Upsilon$
    • (closure) $\forall g, g' \in G_\Upsilon : \forall y \in \Upsilon : (gg')y = gg'y = gy = y \Rightarrow \quad gg' \in G_\Upsilon$
    • (inverse) $\forall g \in G_\Upsilon : \exists g^{-1} \in G : \forall y \in \Upsilon : (g^{-1}g)y = ey = y \Rightarrow \quad (g^{-1}g)y = g^{-1}(gy) = g^{-1}y = y \Rightarrow \quad g^{-1} \in G_\Upsilon$

13. a. (identity) $0 \in G = (\mathbb{R}, +) : \quad \forall \mathbf{x} \in \mathbb{R}^2 : \mathrm{rot}_0\, \mathbf{x} = \mathbf{x}$
    • (associativity) $\forall \theta, \theta' \in G : \forall \mathbf{x} \in \mathbb{R}^2 : \mathrm{rot}_\theta\, \mathrm{rot}_{\theta'}\, \mathbf{x} = \mathrm{rot}_{\theta + \theta'}\, \mathbf{x}$.
    b. The circle centered around the origin containing P.
    c. $G_P = 2\pi\mathbb{Z}$.

14. a. Let $X = \bigcup_i X_i$.
    • (Condition 1) $e \in G : \forall x_i \in X_i : ex_i = x_i \Rightarrow \quad \forall x \in X : ex = x$
    • (Condition 2) $\forall g, g' \in G : \forall x_i \in X_i : (gg')x_i = g(g'x_i) \Rightarrow \quad \forall x \in X : (gg')x = g(g'x)$

b. By Theorem 14, any *G*-set *X* can be partitioned into its orbits.

15. Let $\phi : L \to X : gG_{x_0} \mapsto gx_0$.

- (well-defined) Let $g, g' \in gG_{x_0}$ be elements of the same coset of G_{x_0}. Then $g' \in G_{x_0} \Rightarrow \quad \exists g^* \in G_{x_0} : g' = gg^*$, so $\phi g' = g'x_0 = (gg^*)x_0 = g(g^*x_0) = gx_0 = \phi g$.
- (surjective) Because X is transitive, $\forall x \in X : \exists g \in G : gx_0 = x \Rightarrow \quad \phi(gG_{x_0}) = gx_0 = x$
- (injective) $g'G_{x_0} \neq gG_{x_0} \Rightarrow \quad g^{-1}G_{x_0} \cdot g'G_{x_0} \neq G_{x_0} \Rightarrow \quad g^{-1}g' \notin G_{x_0} \Rightarrow \quad (g^{-1}g')x_0 \neq x_0 \Rightarrow$ $g^{-1}(g'x_0) \neq x_0 \Rightarrow \quad g'x_0 \neq gx_0 \Rightarrow \quad \phi g' \neq \phi g$

So ϕ is an isomorphism from $\left\{_{g\in G} \; gG_{x_0}\right\} \to X$.

16. Every *G*-set is the union of its orbits (Exercise 14b). An orbit is a transitive *G*-set, so every *G*-set is (Exercise 15) isometric to a union of *G*-sets of left cosets in *G*. By the Exercise, this union can be made disjoint.

17. a. $G_{x_0 g_0}$ are the actions $g \in G$ that leave $g_0 x_0$ fixed. If we move $g_0 x_0$ into x_0, act leaving x_0 fixed, and return x_0 to $g_0 x_0$, we have actions that leave $g_0 x_0$ fixed, so $G_{g_0 x_0} \subseteq g_0 G_{x_0} g_0^{-1}$. Conversely, any action that leaves $g_0 x_0$ fixed can be converted into one leaving x_0 fixed, so $G_{x_0} \subseteq g_0^{-1} G_{g_0 x_0} g_0$, from which $g_0 G_{x_0} g_0^{-1} \subseteq G_{g_0 x_0} \Rightarrow \quad G_{x_0 g_0} = g_0 G_{x_0} g_0^{-1}$.

b. It seems reasonable that $H \cong K$ if $\exists g \in G : K = gHg^{-1}$, that is *K* is inner automorphic to *H*, that is (Exercise 3.27) *K* is conjugate to *H*.

c.

§3.6 Applications of *G*-Sets to Counting

1. The group has one permutation that leaves all 8 elements invariant, and 3 others that leave 4 invariant:

$$r = \frac{1}{|G|} +_{g\in G} |X_g| = \tfrac{1}{4}(8 + 3\cdot 4) = \tfrac{20}{4} = 5.$$

2. The group has one permutation that leaves all 8 elements invariant, one (1 3) that leaves 6 invariant, two (2 4 7) and (2 7 4) that leave 5 invariant, and two more that leave only 3 elements invariant:

$$r = \frac{1}{|G|} +_{g\in G} |X_g| = \tfrac{1}{6}(8 + 6 + 2\cdot 5 + 2\cdot 3) = \tfrac{30}{6} = 5.$$

3. *G* is the group of 12 rotations of the tetrahedron, and *X* is the set of 4! markings. The identity rotation leaves all markings invariant; because every face has a different color, every other rotation none:

$$r = \tfrac{1}{12}(4!) = 2.$$

4. *G* is the group of rotations of the cube: there are six ways to fix one face, then four ways to fix a second, so $|G| = 24$. *X* is the set of $8!/2!$ markings. As in the previous exercise, there is only the identity rotation leaving all markings invariant:

$$r = \tfrac{1}{24}\left(\frac{8!}{2!}\right) = 840.$$

5. The identity rotation leaves all 8^6 markings invariant. The 9 rotations that leave a pair of faces invariant can be divided in three groups (rotations along the *x*, *y*, and *z*-axis) of 3 rotations: one of which rotates the cube 180° along the axis, which leaves four independent choices of color for markings that remain invariant under the rotation; and two which rotate the cube 90°, and leave only three independent choices of color. The 8 rotations that leave a pair of opposite vertices invariant are ±120° rotations along the four diagonal axes that leave only two independent choices of face coloring. The 6 rotations that leave a pair of opposite edges invariant are 180° rotations along axes perpendicular to diagonally opposite edges, which leave three independent choices of face coloring:

$$r = \tfrac{1}{24}\left(1\cdot 8^6 + 3\cdot\left(1\cdot 8^4 + 2\cdot 8^3\right) + 8\cdot 8^2 + 6\cdot 8^3\right) = 11712.$$

6. The identity rotation leaves all 4^8 markings invariant. The 3 groups of 9 'face-invariant' rotations each have one 180° rotation leaving four independent colors, and two ±90° rotations leaving two. The 8 'vertex-invariant' rotations leave four independent colors. The 6 'edge-invariant' rotations also leave four:

$$r = \tfrac{1}{24}\left(1 \cdot 4^8 + 3 \cdot \left(1 \cdot 4^4 + 2 \cdot 4^2\right) + 8 \cdot 4^4 + 6 \cdot 4^4\right) = 2916\ .$$

7. The rotations are the fourth dihedral group.

a. Only the identity rotations leaves all markings invariant:

$$r = \tfrac{1}{8}\left(\frac{6!}{2!}\right) = 45\ .$$

b. ρ_0 leaves 4 choices of color, $\rho_{1,3}$ leave one, ρ_2 leaves two, $\mu_{1,2}$ leave three, and $\delta_{1,2}$ leave two:

$$r = \tfrac{1}{8}\left(1 \cdot 6^4 + 2 \cdot 6^1 + 1 \cdot 6^2 + 2 \cdot 6^3 + 2 \cdot 6^2\right) = 231\ .$$

8. The tetrahedron can be rotated by fixing one of four faces and then one of three remaining faces, so $|G| = 12$. The rotation that leaves the first and the second face invariant leaves six independent choices of 'color'. The two rotations that leave the first face invariant and rotates the second leaves two choices. In each of the two remaining groups of rotation for the first face, one leaves the second face invariant and leaves four choices, and two rotate the second face also and leave only once independent choice of 'color':

$$r = \tfrac{1}{12}\left(1 \cdot 2^6 + 2 \cdot 2^2 + 3 \cdot \left(1 \cdot 2^4 + 2 \cdot 2^1\right)\right) = 11\ .$$

9. What is the shape of a prism?

$r = \tfrac{1}{8}\left(6^6 + 1 \cdot 6^4 + 2 \cdot 6^3 + 1 \cdot 6^4 + 1 \cdot 6^3 + 2 \cdot 6^2\right) = 6246$ is not correct.

§4.1 Isomorphism Theorems

♥ 3. Homomorphisms preserve normal subgroups. The Lemma states that, in factor groups at least, this preservation is bijective: there are no more or fewer normal groups containing the factor, then there are in the factor group.

Let $N \triangleleft G$, and $\gamma : G \to G/N$ the canonical homomorphism. Then, the canonical correspondence ϕ given by $\phi : L \to \gamma L$ between normal groups containing N in G, and normal groups in G/N is bijective.

Note the fact that we have two names γ and ϕ for essentially the same operation. γ operates on elements h to produce $\gamma(h)$, but has an implicit 'extended' interpretation in which it operates on sets H to produce $\gamma[H] \equiv \cup_{h \in H}\, \gamma(h)$. ϕ is simply a name given to this interpretation. The book uses the special notation with square brackets to indicate the extended interpertation.

First, show that ϕ is well-defined. If $L \triangleleft G$ ($L \supseteq N$ is not really relevant here), and $\gamma : G \to G/N$ is a homomorphism, then by Theorem 3.3.16 $\phi L = \gamma L \triangleleft G/N$, so ϕ really does produce normal groups.

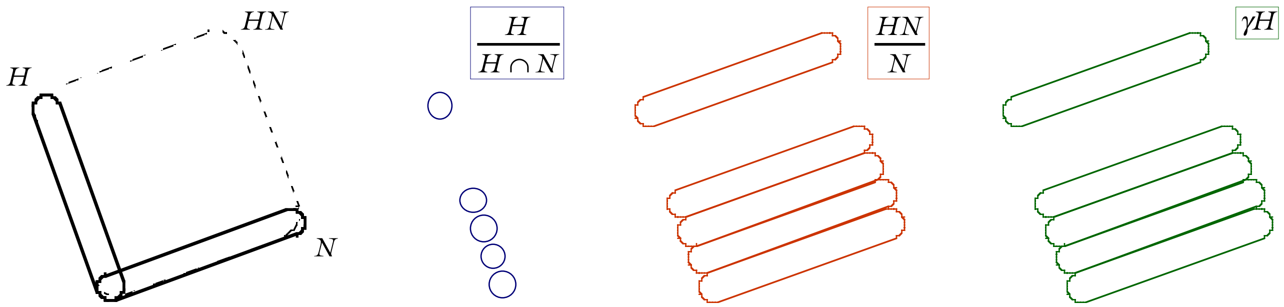
To show that ϕ is injective we need to be able to calculate inverses. By Theorem 3.1.15, the inverse of the forward homomorphism of an element is the coset of its kernel containing that element, i.e. inverses of forward mappings of elements $g \in G$ under γ are of the form $g\,\mathrm{Ker}\,\gamma$. Let $L \triangleleft G, L \supseteq N$. Since $\mathrm{Ker}\,\gamma = N \subseteq L$ and L is a subgroup and thus closed, $\forall g \in L$: $g\,\mathrm{Ker}\,\gamma \subseteq L$, so $L\,\mathrm{Ker}\,\gamma \subseteq L$. Conversely, $\forall g \in L$: $g \in g\,\mathrm{Ker}\,\gamma$ so $L \subseteq L\,\mathrm{Ker}\,\phi$, so $L\,\mathrm{Ker}\,\phi = L \Rightarrow \quad L = \gamma^{-1}\gamma L = \gamma^{-1}\phi L.$

Now, show that ϕ is injective. Let $L, M \triangleleft G$ such that $\phi L = \phi M.$ Then from the above, $L = \gamma^{-1}\phi L$ and $M = \gamma^{-1}\phi M = \gamma^{-1}\phi L$ so $L = M.$

Finally, show that ϕ is surjective. Let $H \triangleleft G/N$, then $\gamma^{-1}H \subseteq G : \phi\gamma^{-1}H = \gamma\gamma^{-1}H = H$, $\gamma^{-1}H \supseteq N$ and normal in G by Theorem 3.3.16.

♥ 5. Given a homomorphism, Theorem 2 allows us to generate isomorphisms between the image of that homomorphism and a factor group. Applying this procedure twice, this allows us to generate isomorphisms between factor groups. Note that it is not even necessary to consider the canonical homomorphism γ (the missing side of the triangles in the diagram).

$$\begin{tikzcd} & H \arrow[dr, "\begin{array}{l}\gamma\mid_H \text{ homomorphism}\\ \operatorname{Ker}\gamma\mid_H = H\cap N\end{array}"] & \\ \boxed{\dfrac{H}{H\cap N}} \arrow[rr, "\mu_1 \text{ isomorphism}"'] & & \boxed{\gamma H}\end{tikzcd} \qquad \begin{tikzcd} & HN \arrow[dr, "\begin{array}{l}\gamma\mid_{HN} \text{ homomorphism}\\ \operatorname{Ker}\gamma\mid_{HN} = N\end{array}"] & \\ \boxed{\dfrac{HN}{N}} \arrow[rr, "\mu_2 \text{ isomorphism}"'] & & \boxed{\gamma H}\end{tikzcd}$$



1. a. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3 : i \mapsto 2i \bmod 3$; $\phi 1 = 2$. $\operatorname{Ker}\phi = \frac{3}{2}\mathbb{Z} \cap \mathbb{Z}_{12}$.

   b. $\{0,3,6,9\}, \{1,4,7,10\}, \{2,5,8,11\}$.

   c. $\mu : \mathbb{Z}_{12}/K \to \mathbb{Z}_3 : \operatorname{Ker}\phi + i \mapsto i$.

2. a. $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_{12} : i \mapsto 10i \bmod 12$; $\phi 1 = 10$. $\operatorname{Ker}\phi = \frac{12}{10}\mathbb{Z} \cap \mathbb{Z}_{18} = \{0,6,12\}$.

   b. $\{0,6,12\}, \{1,7,13\}, \{2,8,14\}, \{3,9,15\}, \{4,10,16\}, \{5,11,17\}$.

   c. By Theorem 2 it is isomorphic to $\mathbb{Z}_{18}/\operatorname{Ker}\phi \cong \mathbb{Z}_{18}/\mathbb{Z}_3 \cong \mathbb{Z}_6$.

   d. $\mu : \mathbb{Z}_{18} \to \phi\mathbb{Z}_{18} : \operatorname{Ker}\phi + i \mapsto i$.

3. $H = \langle 4 \rangle_{\mathbb{Z}_{24}} = \{0,4,8,12,16,20\}$, $N = \langle 6 \rangle_{\mathbb{Z}_{24}} = \{0,6,12,18\}$.

   a. $HN = \{0,2,4,\ldots,22\}$, $H \cap N = \{0,12\}$.

   b. $\dfrac{HN}{N} = \{\{0,6,12,18\},\{2,8,14,20\},\{4,10,16,22\}\}$.

   c. $\dfrac{H}{H \cap N} = \{\{0,12\},\{4,16\},\{8,20\}\}$.

   d. $\phi : \dfrac{HN}{N} \to \dfrac{H}{H \cap N} : N + i \mapsto (H \cap N) + 2i$.

   Note that the book gives a different correspondence. This is possible because $\mathbb{Z}_3$ is automorphic.

4. $H = \langle 6 \rangle_{\mathbb{Z}_{36}} = \{0,6,12,18,24\}$; $N = \langle 9 \rangle_{\mathbb{Z}_{36}} = \{0,9,18,27\}$.

   a. $HN = \{0,3,6,\ldots,33\}$, $H \cap N = \{0,18\}$.

   b. $\dfrac{HN}{N} = \{\{0,9,18,27\},\{3,12,21,30\},\{6,15,24,33\}\}$.

   c. $\dfrac{H}{H \cap N} = \{\{0,18\},\{6,24\},\{12,30\}\}$.

   d. $\phi : \dfrac{HN}{N} \to \dfrac{H}{H \cap N} : N + i \mapsto (H \cap N) + 2i$.

5. $H = \langle 4 \rangle_{\mathbb{Z}_{24}} = \{0,4,8,\ldots,20\}$; $K = \langle 8 \rangle_{\mathbb{Z}_{24}} = \{0,8,16\}$.

a. $\dfrac{G}{H} = \{\{0,4,8,12,16,20\},\{1,5,9,13,17,21\},\{2,6,10,14,18,22\},\{3,7,11,15,19,23\}\}$.

b. $\dfrac{G}{K} = \{\{0,8,16\},\{1,9,17\},\{2,10,18\},\{3,11,19\},\{4,12,20\},\{5,13,21\},\{6,14,22\},\{7,15,23\}\}$.

c. $\dfrac{H}{K} = \{\{0,8,16\},\{4,12,20\}\}$.

d. $\dfrac{G/K}{H/K} = \{\{\{0,8,16\},\{4,12,20\}\},\quad \{\{1,9,17\},\{5,13,21\}\},\quad \{\{2,10,18\},\{6,14,22\}\},\quad \{\{3,11,19\},\{7,15,23\}\}\}$.

e. $\phi : \dfrac{G}{H} \to \dfrac{G/K}{H/K} : H + i \mapsto (H/K) + i$.

Note that the book writes the correspondence as $i \mapsto (H/K) + (K + i)$. This gives the same sets using a different computation.

6. $H = \langle 9 \rangle_{\mathbb{Z}_{36}} = \{0,9,18,27\}$; $K = \langle 18 \rangle_{\mathbb{Z}_{36}} = \{0,18\}$.

a. $\dfrac{G}{H} = \left\{\begin{array}{l} \{0,9,18,27\},\{1,10,19,28\},\{2,11,20,29\}, \\ \{3,12,21,30\},\{4,13,22,31\},\{5,14,23,32\}, \\ \{6,15,24,33\},\{7,16,25,34\},\{8,17,26,35\} \end{array}\right\}$.

b. $\dfrac{G}{K} = \left\{\begin{array}{l} \{0,18\},\{1,19\},\{2,20\},\{3,21\},\{4,22\},\{5,23\},\{6,24\},\{7,25\},\{8,26\}, \\ \{9,27\},\{10,28\},\{11,29\},\{12,30\},\{13,31\},\{14,32\},\{15,33\},\{16,34\},\{17,35\} \end{array}\right\}$.

c. $\dfrac{H}{K} = \{\{0,18\},\{9,27\}\}$.

d. $\dfrac{G/K}{H/K} = \left\{\begin{array}{lll} \{\{0,18\},\{9,27\}\}, & \{\{1,19\},\{10,28\}\}, & \{\{2,20\},\{11,29\}\}, \\ \{\{3,21\},\{12,30\}\}, & \{\{4,22\},\{13,31\}\}, & \{\{5,23\},\{14,32\}\}, \\ \{\{6,24\},\{15,33\}\}, & \{\{7,25\},\{16,34\}\}, & \{\{8,26\},\{17,35\}\} \end{array}\right\}$.

e. $\phi : \dfrac{G}{H} \to \dfrac{G/K}{H/K} : H + i \mapsto (H/K) + i$.

7. $H : \underset{H_0}{\{0\}} \subset \underset{H_1}{\langle 12 \rangle} \subset \underset{H_2}{\langle 3 \rangle} \subset \underset{H_3}{\mathbb{Z}_{36}}$; $K : \underset{K_0}{\{0\}} \subset \underset{K_1}{\langle 18 \rangle} \subset \underset{K_2}{\mathbb{Z}_{36}}$.

$H_{00} = H_0(H_1 \cap K_0) = E(\langle 12 \rangle \cap E) = EE = E$

$H_{01} = H_0(H_1 \cap K_1) = E(\langle 12 \rangle \cap \langle 18 \rangle) = EE = E$

$H_{02} = H_0(H_1 \cap K_2) = E(\langle 12 \rangle \cap \mathbb{Z}_{36}) = E\langle 12 \rangle = \langle 12 \rangle$

$H_{10} = H_1(H_2 \cap K_0) = \langle 12 \rangle(\langle 3 \rangle \cap E) = \langle 12 \rangle E = \langle 12 \rangle$

$H_{11} = H_1(H_3 \cap K_1) = \langle 12 \rangle(\langle 3 \rangle \cap \langle 18 \rangle) = \langle 12 \rangle\langle 18 \rangle = \langle 6 \rangle$

$H_{12} = H_2(H_3 \cap K_2) = \langle 12 \rangle(\langle 3 \rangle \cap \mathbb{Z}_{36}) = \langle 12 \rangle\langle 3 \rangle = \langle 3 \rangle$

$H_{20} = H_2(H_3 \cap K_0) = \langle 3 \rangle(\mathbb{Z}_{36} \cap E) = \langle 3 \rangle E = \langle 3 \rangle$

$H_{21} = H_2(H_3 \cap K_1) = \langle 3 \rangle(\mathbb{Z}_{36} \cap \langle 18 \rangle) = \langle 3 \rangle\langle 18 \rangle = \langle 3 \rangle$

$H_{22} = H_3(H_3 \cap K_2) = \langle 3 \rangle(\mathbb{Z}_{36} \cap \mathbb{Z}_{36}) = \langle 3 \rangle\mathbb{Z}_{36} = \mathbb{Z}_{36}$

and

$K_{00} = K_0(K_1 \cap H_0) = E(\langle 18\rangle \cap E) = EE = E$

$K_{01} = K_0(K_1 \cap H_1) = E(\langle 18\rangle \cap \langle 12\rangle) = EE = E$

$K_{02} = K_0(K_1 \cap H_2) = E(\langle 18\rangle \cap \langle 3\rangle) = E\langle 18\rangle = \langle 18\rangle$

$K_{03} = K_0(K_1 \cap H_3) = E(\langle 18\rangle \cap \mathbb{Z}_{36}) = E\langle 18\rangle = \langle 18\rangle$

$K_{10} = K_1(K_2 \cap H_0) = \langle 18\rangle(\mathbb{Z}_{36} \cap E) = \langle 18\rangle E = \langle 18\rangle$

$K_{11} = K_1(K_2 \cap H_1) = \langle 18\rangle(\mathbb{Z}_{36} \cap \langle 12\rangle) = \langle 18\rangle\langle 12\rangle = \langle 6\rangle$

$K_{12} = K_2(K_2 \cap H_2) = \langle 18\rangle(\mathbb{Z}_{36} \cap \langle 3\rangle) = \langle 18\rangle\langle 3\rangle = \langle 3\rangle$

$K_{13} = K_2(K_2 \cap H_3) = \langle 18\rangle(\mathbb{Z}_{36} \cap \mathbb{Z}_{36}) = \langle 18\rangle\mathbb{Z}_{36} = \mathbb{Z}_{36}$

This gives the chains

$$\begin{array}{llll} E & = E & \subseteq E & \subseteq \langle 12\rangle \\ & \subseteq \langle 12\rangle & \subseteq \langle 6\rangle & \subseteq \langle 3\rangle \\ & \subseteq \langle 3\rangle & \subseteq \langle 3\rangle & \subseteq \mathbb{Z}_{36} \quad = \mathbb{Z}_{36} \end{array} \quad \text{and} \quad \begin{array}{lllll} E & = E & \subseteq E & \subseteq \langle 18\rangle & \subseteq \langle 18\rangle \\ & \subseteq \langle 18\rangle & \subseteq \langle 6\rangle & \subseteq \langle 3\rangle & \subseteq \mathbb{Z}_{36} \quad = \mathbb{Z}_{36} \end{array},$$

or $E \subset \langle 12\rangle \subset \langle 6\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{36}$; $\quad E \subset \langle 18\rangle \subset \langle 6\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{36}$.

The factor group isomorphisms are:

A: $\quad \langle 12\rangle/E \cong \langle 6\rangle/\langle 18\rangle \cong \mathbb{Z}_3$

B: $\quad \langle 6\rangle/\langle 12\rangle \cong \langle 18\rangle/E \cong \mathbb{Z}_2$

C: $\quad \langle 3\rangle/\langle 6\rangle \cong \langle 3\rangle/\langle 6\rangle \cong \mathbb{Z}_2$

D: $\quad \mathbb{Z}_{36}/\langle 3\rangle \cong \mathbb{Z}_{36}/\langle 3\rangle \cong \mathbb{Z}_3$

8. $\quad H: \underset{H_0}{\{0\}} \subseteq \underset{H_1}{\langle 12\rangle} \subseteq \underset{H_2}{\langle 4\rangle} \subseteq \underset{H_3}{\mathbb{Z}_{24}}; \quad K: \underset{K_0}{\{0\}} \subseteq \underset{K_1}{\langle 6\rangle} \subseteq \underset{K_2}{\langle 3\rangle} \subseteq \underset{K_3}{\mathbb{Z}_{24}}$

$H_{00} = H_0(H_1 \cap K_0) = E(\langle 12\rangle \cap E) = EE = E$

$H_{01} = H_0(H_1 \cap K_1) = E(\langle 12\rangle \cap \langle 6\rangle) = E\langle 12\rangle = \langle 12\rangle$

$H_{02} = H_0(H_1 \cap K_2) = E(\langle 12\rangle \cap \langle 3\rangle) = E\langle 12\rangle = \langle 12\rangle$

$H_{03} = H_0(H_1 \cap K_3) = E(\langle 12\rangle \cap \mathbb{Z}_{24}) = E\langle 12\rangle = \langle 12\rangle$

$H_{10} = H_1(H_2 \cap K_0) = \langle 12\rangle(\langle 4\rangle \cap E) = \langle 12\rangle E = \langle 12\rangle$

$H_{11} = H_1(H_2 \cap K_1) = \langle 12\rangle(\langle 4\rangle \cap \langle 6\rangle) = \langle 12\rangle\langle 12\rangle = \langle 12\rangle$

$H_{12} = H_1(H_3 \cap K_2) = \langle 12\rangle(\langle 4\rangle \cap \langle 3\rangle) = \langle 12\rangle\langle 12\rangle = \langle 12\rangle$

$H_{13} = H_1(H_4 \cap K_3) = \langle 12\rangle(\langle 4\rangle \cap \mathbb{Z}_{24}) = \langle 12\rangle\langle 4\rangle = \langle 4\rangle$

$H_{20} = H_2(H_3 \cap K_0) = \langle 4\rangle(\mathbb{Z}_{24} \cap E) = \langle 4\rangle E = \langle 4\rangle$

$H_{21} = H_3(H_4 \cap K_1) = \langle 4\rangle(\mathbb{Z}_{24} \cap \langle 6\rangle) = \langle 4\rangle\langle 6\rangle = \langle 2\rangle$

$H_{22} = H_3(H_4 \cap K_2) = \langle 4\rangle(\mathbb{Z}_{24} \cap \langle 3\rangle) = \langle 4\rangle\langle 3\rangle = \langle 1\rangle = \mathbb{Z}_{24}$

$H_{23} = H_3(H_4 \cap K_3) = \langle 4\rangle(\mathbb{Z}_{24} \cap \mathbb{Z}_{24}) = \langle 4\rangle\mathbb{Z}_{24} = \mathbb{Z}_{24}$

and

$K_{00} = K_0(K_1 \cap H_0) = E(\langle 6\rangle \cap E) = EE = E$

$K_{01} = K_0(K_1 \cap H_1) = E(\langle 6\rangle \cap \langle 12\rangle) = E\langle 12\rangle = \langle 12\rangle$

$K_{02} = K_0(K_1 \cap H_2) = E(\langle 6\rangle \cap \langle 4\rangle) = E\langle 12\rangle = \langle 12\rangle$

$K_{03} = K_0(K_1 \cap H_3) = E(\langle 6\rangle \cap \mathbb{Z}_{24}) = E\langle 6\rangle = \langle 6\rangle$

$$
\begin{aligned}
K_{10} &= K_1(K_2 \cap H_0) = \langle 6\rangle(\langle 3\rangle \cap E) = \langle 6\rangle E = \langle 6\rangle\\
K_{11} &= K_1(K_2 \cap H_1) = \langle 6\rangle(\langle 3\rangle \cap \langle 12\rangle) = \langle 6\rangle\langle 12\rangle = \langle 6\rangle\\
K_{12} &= K_2(K_3 \cap H_2) = \langle 6\rangle(\langle 3\rangle \cap \langle 4\rangle) = \langle 6\rangle\langle 12\rangle = \langle 6\rangle\\
K_{13} &= K_3(K_3 \cap H_3) = \langle 6\rangle(\langle 3\rangle \cap \mathbb{Z}_{24}) = \langle 6\rangle\langle 3\rangle = \langle 3\rangle\\
K_{20} &= K_2(K_3 \cap H_0) = \langle 3\rangle(\mathbb{Z}_{24} \cap E) = \langle 3\rangle E = \langle 3\rangle\\
K_{21} &= K_2(K_3 \cap H_1) = \langle 3\rangle(\mathbb{Z}_{24} \cap \langle 12\rangle) = \langle 3\rangle\langle 12\rangle = \langle 3\rangle\\
K_{22} &= K_2(K_3 \cap H_2) = \langle 3\rangle(\mathbb{Z}_{24} \cap \langle 4\rangle) = \langle 3\rangle\langle 4\rangle = \langle 1\rangle = \mathbb{Z}_{24}\\
K_{23} &= K_3(K_3 \cap H_3) = \langle 3\rangle(\mathbb{Z}_{24} \cap \mathbb{Z}_{24}) = \langle 3\rangle\mathbb{Z}_{24} = \mathbb{Z}_{24}
\end{aligned}
$$

This gives the chains

$$
\begin{array}{lllll}
E & = E & \subseteq\langle 12\rangle & \subseteq\langle 12\rangle & \subseteq\langle 12\rangle\\
 & \subseteq\langle 12\rangle & \subseteq\langle 12\rangle & \subseteq\langle 12\rangle & \subseteq\langle 4\rangle\\
 & \subseteq\langle 4\rangle & \subseteq\langle 2\rangle & \subseteq\mathbb{Z}_{24} & \subseteq\mathbb{Z}_{24} \quad = \mathbb{Z}_{24}
\end{array}
\quad \text{and} \quad
\begin{array}{lllll}
E & = E & \subseteq\langle 12\rangle & \subseteq\langle 12\rangle & \subseteq\langle 6\rangle\\
 & \subseteq\langle 6\rangle & \subseteq\langle 6\rangle & \subseteq\langle 6\rangle & \subseteq\langle 3\rangle\\
 & \subseteq\langle 3\rangle & \subseteq\langle 3\rangle & \subseteq\mathbb{Z}_{24} & \subseteq\mathbb{Z}_{24} \quad = \mathbb{Z}_{24}
\end{array}
\quad ,
$$

or $E \subset \langle 12\rangle \subset \langle 4\rangle \subset \langle 2\rangle \subset \mathbb{Z}_{24}$; $E \subset \langle 12\rangle \subset \langle 6\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{24}$.

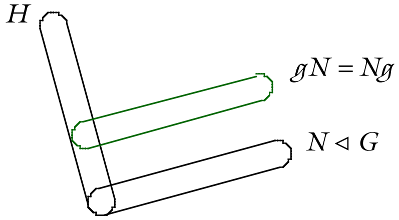
The factor group isomorphisms are:

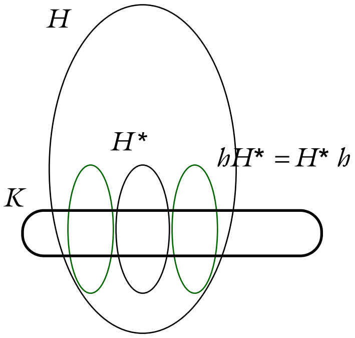
A : $\langle 12\rangle / E \cong \langle 12\rangle / E \cong \mathbb{Z}_2$

B : $\langle 4\rangle / \langle 12\rangle \cong \mathbb{Z}_4 / \langle 3\rangle \cong \mathbb{Z}_3$

C : $\langle 2\rangle / \langle 4\rangle \cong \langle 6\rangle / \langle 12\rangle \cong \mathbb{Z}_2$

D : $\mathbb{Z}_{24} / \langle 2\rangle \cong \langle 3\rangle / \langle 6\rangle \cong \mathbb{Z}_2$





9. (left figure) Because H is a group, $\forall h \in H: h(H \cap N) \in H$. Also, obviously $h(N \setminus H \cap N) \notin H$, so $h(H \cap N) = hN \cap H$. Similarly, $(H \cap N)h = Nh \cap H$. Because $N \lhd G$, $hN = Nh$, so $h(H \cap N) = (H \cap N)h$ and so $H \cap N \lhd H$.

10. (right figure) Let $h \in H \cap K$. Then $h(H^* \cap K) \in hH^* \cap K$. Also, obviously $\forall h' \in H \setminus H \cap K: h'(H^* \cap K) \notin hH^* \cap K$, so $h(H^* \cap K) = hH^* \cap K$. Similarly, $(H^* \cap K)h = H^* h \cap K$. Because $H^* \lhd H$, $h(H^* \cap K) = (H^* \cap K)h$, so $H^* \cap K \lhd H \cap K$.

11. a. Prove that $K/H \lhd G/H$. Now, this is the case if $\forall gH \in G/H, kH \in K/H: gH \cdot kH \cdot (gH)^{-1} \in K/H$. Since coset multiplication is well-defined by $H \lhd G$, this is true if $(gkg^{-1})H \in K/H$ or $gkg^{-1} \in K$, which is just to say that $K \lhd G$. The same argument proves $L/H \lhd G/H$.
Inclusion follows immediately from $K \subset L \Rightarrow \quad \exists l \in L \setminus K: lH \in L/H, lH \notin K/H \Rightarrow \quad K/H \subset L/H$.

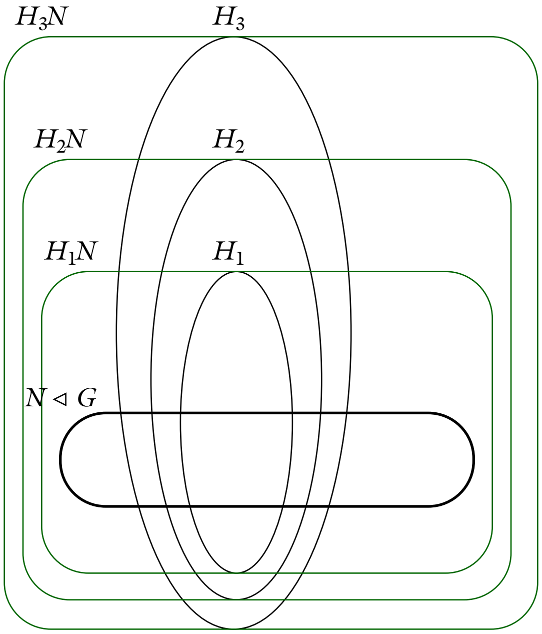
b. Because $B,C \lhd A$, $B \subset C$, by the Third Isomorphism Theorem $\dfrac{A/B}{C/B} \cong A/C$, or writing the synonyms out,

$\left.\dfrac{G/H}{K/H}\middle/\dfrac{\dfrac{L/H}{K/H}}{}\right. \cong \dfrac{G/H}{L/H} \cong G/L$. This exercise proves a sort of 'transitivity' of the Third Isomorphism Theorem.

12. By Lemma 4, $K \cup L = KL = G$, so by the Second Isomorphism Theorem $\dfrac{KL}{L} \cong \dfrac{K}{K \cap L} \Rightarrow \quad \dfrac{G}{L} \cong \dfrac{K}{E} = K$. Mutatis mutandis G/K.

13. Since G is solvable, there is a maximal $\left({}_i\ G_i\right)$ such that $G_i \triangleleft G_{i+1}$ and $G_{i+1} \big/ G_i$ commutative. By Exercise 10, $K \cap G_i \triangleleft K \cap G_{i+1}$, so $\left({}_i\ K \cap G_i\right)$ forms a subnormal series. I don't know by what argument the factor groups are simple, so that this is also a composition series. G_i are commutative, and thus so are $K \cap G_i$ and $K \cap G_{i+1} \big/ K \cap G_i$. So $K \cap G$ is solvable.

14. (See figure) $\left({}_i\ H_iN\right)$ is a composition series iff it is a subnormal series with simple factors. Obviously $H_0N = E \triangleleft H_1N$. For all other subgroups in the series, $\forall hn \in H_{i+1}N : (hn)(H_iN) \overset{H_i \triangleleft H_{i+1}}{=} H_i(hn)N \overset{N \triangleleft G}{=} (H_iN)(hn)$ so $H_i \triangleleft H_{i+1}$ and the series is subnormal. To see that the factor groups are simple, we evaluate $\dfrac{H_{i+1}N}{H_iN} = \dfrac{H_{i+1} \cdot H_iN}{H_iN} \overset{\text{2 Iso Th}}{\cong} \dfrac{H_{i+1}}{H_{i+1} \cap H_iN} \overset{\text{3 Iso Th}}{\cong} \dfrac{H_{i+1}/H_i}{\left(H_{i+1} \cap H_iN\right)/H_i}$. Now H_{i+1}/H_i is simple, so the denominator must be either trivial or nonproper. Obviously $H_i \subset H_{i+1} \Rightarrow \quad H_{i+1} \cap H_iN \subset H_{i+1}$, so the denominator is proper and must therefore be trivial. So the fraction as a whole is isomorphic to just H_{i+1}/H_i, and thus the factor groups of our series are simple also.



15. (See figure relating to Exercise 14, repacing H_iN with H_i/N) $\left({}_i\ H_i/N\right)$ is a composition series iff it is a subnormal series with simple factors. $H_i/N \triangleleft H_{i+1}/N$ iff $\forall hN \in H_{i+1}/N : hN\left(H_i/N\right) = \left(H_i/N\right)hN$.

$$H_i \triangleleft H_{i+1} \quad \Rightarrow hH_i = H_ih \quad \Rightarrow hH_i \cdot N = H_ih \cdot N \quad \overset{N \triangleleft G}{\Rightarrow} hN \cdot H_i = H_i \cdot hN \quad \overset{\substack{\text{canonical}\\ \text{homomorphism}}}{\Rightarrow} \quad \frac{hN \cdot H_i}{N} = \frac{H_i \cdot hN}{N}$$

$$\overset{\substack{\text{coset multiplication}\\ \text{well-defined}}}{\Rightarrow} \qquad hN \cdot H_i/N = H_i/N \cdot hN$$

so the series is indeed subnormal. To see that the factor groups are simple, we first find that $\dfrac{H_{i+1}/N}{H_i/N} \cong \dfrac{H_{i+1}N}{H_iN}$ (*) which (we saw in Exercise 14) is simple. The isomorphism follows from the fact that

$\psi_i : H_{i+1}N \to \dfrac{H_{i+1}/N}{H_i/N} : hn \mapsto hN \cdot (H_i/N)$ is a homomorphism:

$$\forall hn, h'n' \in H_{i+1}N: \quad \psi_i(hn)\cdot\psi_i(h'n') = (hN\cdot(H_i/N))\cdot(h'N\cdot(H_i/N)) = hN\cdot h'N\cdot(H_i/N) =$$
$$hh'N\cdot(H_i/N) = \psi_i(hn\cdot h'n')$$

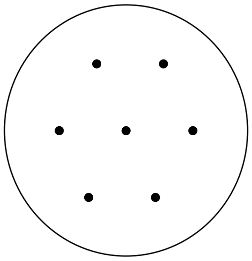
By the First Isomorphism Theorem, the range of the homomorphism is isomorphic to the kernel factor group of the range, which is the beforementioned (*) isomorphism above.

16. Let G be solvable by $({}_i\ G_i)$, and ϕ be a homomorphism. By the First Isomorphism Theorem, $\phi G \cong G/\mathrm{Ker}\,\phi$. Then by Exercise 15, $G/\mathrm{Ker}\,\phi$ has a composition series also in the distinct groups of $({}_i\ G_i/\mathrm{Ker}\,\phi)$. Since G_{i+1}/G_i are commutative, then so are $G_{i+1}/\mathrm{Ker}\,\phi \big/ G_i/\mathrm{Ker}\,\phi$. So $G/\mathrm{Ker}\,\phi$ and ϕG are solvable.

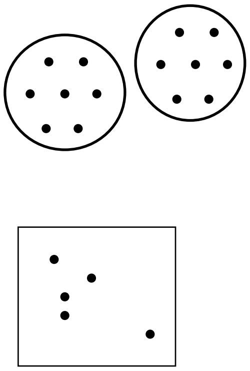
§4.2 Sylow Theorems

♥ The normalizer $N_G H$ is the largest subgroup of G in which H is normal.

♥ 1. This theorem applies the obvious fact that when a G-set X is stripped of its 'irrelevant' part, the remainder reflects something of the structure of the group. In particular, if G is a p-group, the important part of X has a multiple of p elements.



p-group G



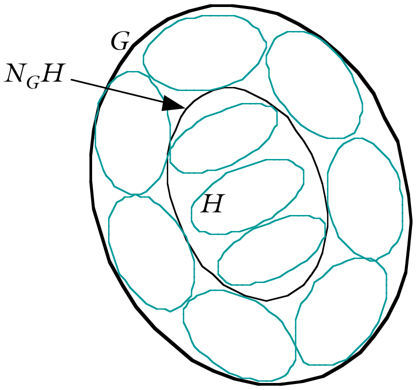
orbits of X
This is the 'important' part of X that actually says something about G
$|X| - |X_G| \in \mathbb{N}p$

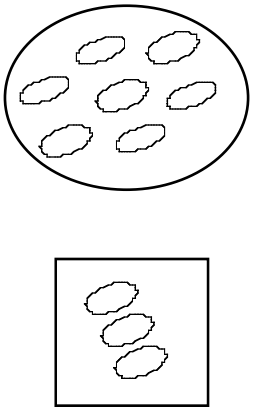
X_G
This is the 'irrelevant' part of X that is invariant for all g and says nothing about G

G-set X

♥ 3. This applies the previous theorem. The entire X also has a multiple of p elements, so we can conclude that the irrelevant part does too. That irrelevant part happens to consist of p-tuples of one single element, and because there is at least one, there have to be at least p.

♥ 6. Now the theorem leads to conclude that there is a multiple of p cosets of H outside of the normalizer.





♥ 8. Since there is a multiple of p cosets of H in the whole of G, and (by Lemma 6) a multiple outside of the normalizer, there must be a multiple of p inside it as well. Inside the normalizer, we can then find one that has exactly p, and if H is of order p^i, this new one will form a subgroup of order p^{i+1}.

1. $12 = 2^2 \cdot 3^1$, so by the remark following Definition 9 the maximal 3-subgroups have order $3^1 = 3$.

2. $54 = 2 \cdot 3^3$, so the maximal 3-subgroups have order $3^3 = 27$.

3. By the Third Sylow Theorem, the number must be in $\left(2\mathbb{N}+1\right) \cap \left\{1, 2, 3, 4, 6, 8, 12\right\} = \left\{1, 3\right\}$.

4. The number must be in $\left(3\mathbb{N}+1\right) \cap \left\{1,\ 3,\ 5,\ 17,\ 3 \cdot 5 = 15,\ 3 \cdot 17 = 51,\ 5 \cdot 17 = 85,\ 3 \cdot 5 \cdot 17 = 255\right\} = \left\{1, 85\right\}$.

5. $\left|S_4\right| = 4! = 24 = 2^3 3^1$, so a maximal 3-subgroup has order $3^1 = 3$. There are $\left(3\mathbb{N}+1\right) \cap \left\{1, 2, 3, 4, 6, 8, 12\right\} = \left\{1, 4\right\}$ of them. Now $\left\langle \left(1\ 2\ 3\right) \right\rangle = \left\{\left(\ \right), \left(1\ 2\ 3\right), \left(1\ 3\ 2\right)\right\}$ is a 3-subgroup and maximal, and so are the other three 3-cycles. By example, $\left\langle \left(1\ 2\ 4\right) \right\rangle$ is conjugate by $\left(3\ 4\right)$:

   $\left(3\ 4\right)^{-1}\left(\ \right)\left(3\ 4\right) = \left(\ \right)$; $\quad \left(3\ 4\right)^{-1}\left(1\ 2\ 3\right)\left(3\ 4\right) = \left(1\ 2\ 4\right)$; $\quad \left(3\ 4\right)^{-1}\left(1\ 3\ 2\right)\left(3\ 4\right) = \left(1\ 4\ 2\right)$.

   The rest follow similarly.

6. The order of a maximal 2-subgroup of S_4 is (Exercise 5) $2^3 = 8$, and there are (Exercise 3) either 1 or 3 of them. There are $4!/0! \cdot 4 = 6$ 4-cycles, $4!/1! \cdot 3 = 8$ 3-cycles, $4!/2! \cdot 2 = 6$ 2-cycles, $4!/4 \cdot 2 = 3$ 2×2-cycles, and 1 1-cycle. The 3-cycles have order 3 and cannot participate in 2-subgroups. Every subgroup must contain the 1-cycle identity. Conjecture that the remaining 7 elements of each of the three 2-subgroups result from some 'symmetric' distribution of the 4-, 2-, and 2×2-cycles. One such distribution is to assign all 3 2×2-cycles, and one-third each of the 4- and 2-cycles to each 2-subgroup. Since the 1- and 2×2-cycles are the only even permutations, they are closed in each subgroup. It remains to be shown that the product of any odd and even permutation results in one of the four odd 4- and 2-cycles from its distribution. Assign to a 2-subgroups the two component 2-cycles from one of the 2×2-cycles, for example, (1 2) and (3 4):

   $(1\ \ 2)(3\ \ 4) \cdot (1\ \ 2) = (3\ \ 4), \quad (1\ \ 2)(3\ \ 4) \cdot (3\ \ 4) = (1\ \ 2)$

   $(1\ \ 3)(2\ \ 4) \cdot (1\ \ 2) = (1\ \ 4\ \ 2\ \ 3), \quad (1\ \ 3)(2\ \ 4) \cdot (3\ \ 4) = (1\ \ 3\ \ 2\ \ 4)$

   $(1\ \ 4)(2\ \ 3) \cdot (1\ \ 2) = (1\ \ 3\ \ 2\ \ 4), \quad (1\ \ 4)(2\ \ 3) \cdot (3\ \ 4) = (1\ \ 4\ \ 2\ \ 3)$

   Hence the two 4-cycles that need to be distributed to the 2-subgroup follow naturally. Note that the two 2- and 4-cycles are each others' inverses, so the entire 2-subgroup is closed and thus well-defined.

   The other two 2-subgroups follow directly from mechanical substitution of letters in the permutations.

   To show conjugacy, note first that the subgroup of even cycles (which is contained by each 2-subgroup) is normal. Finally, verify that the odd cycles of one 2-subgroup are conjugate to those in another under one of the 3-cycles:

   $(1\ \ 2\ \ 3)^{-1} \cdot (1\ \ 2) \cdot (1\ \ 2\ \ 3) = (1\ \ 3); \quad (1\ \ 2\ \ 3)^{-1} \cdot (1\ \ 3\ \ 2\ \ 4) \cdot (1\ \ 2\ \ 3) = (1\ \ 4\ \ 3\ \ 2);$

   $(1\ \ 2\ \ 3)^{-1} \cdot (3\ \ 4) \cdot (1\ \ 2\ \ 3) = (2\ \ 4); \quad (1\ \ 2\ \ 3)^{-1} \cdot (1\ \ 4\ \ 2\ \ 3) \cdot (1\ \ 2\ \ 3) = (1\ \ 2\ \ 3\ \ 4).$

7. "order power of *p*"

8. "the maximal set of elements by whose inner automorphisms"

9. Correct— this uses Corollary 4.

10. a. true (by the Third Sylow Theorem)
   b. true (by Example 13)
   c. true (by Corollary 4)
   d. false (a 2-subgroup of a group of order 2^2 could have order 2^1)
   e. true (any subgroup of a commutative group is invariant under conjugation)
   f. false?
   g. true (Definition 5)
   h. true (by the Second Sylow Theorem all maximal *p*-subgroups are conjugate and thus not invariant)
   i. false (for a commutative group $N_G H = G$)
   j. false (but it is true that it has no *proper* *p*-subgroup)

11. (closure) $\forall g, g' \in G_H : \left(gg'\right)H\left(gg'\right)^{-1} = gg'Hg'^{-1}g^{-1} \overset{g' \in G_H}{=} gHg^{-1} \overset{g \in G_H}{=} H \quad \Rightarrow gg' \in G_H$.

   (identity) $e \in G : \quad eHe^{-1} = H \quad \Rightarrow e \in G_H$.

   (inverse) $\forall g \in G_H : \quad gHg^{-1} = H \quad \Rightarrow Hg^{-1} = g^{-1}H \quad \Rightarrow H = g^{-1}Hg = g^{-1}H\left(g^{-1}\right)^{-1} \quad \Rightarrow g^{-1} \in G_H$.

12. By the Second Sylow Theorem, all maximal *p*-subgroups are conjugate. If *G* has only one such subgroup, then it must therrefore be invariant under conjugacy, which is to say, it is a normal subgroup. Assuming that $\left|G\right| \notin p^{\mathbb{N}}$, this subgroup is proper; and assuming that $p > 1$, it is not trivial. Then *G* is not simple.

13. $45 = 3^2 5^1$, so the maximal 3-subgroups of such a group have order $3^2 = 9$ and their number is in $\left(3\mathbb{N}+1\right) \cap \left\{1, 3, 5, 9, 15, 45\right\} = \left\{1\right\}$. So by Exercise 12 the subgroup is normal.

14. If a group is divisible by a prime other than *p*, then by Cauchy it has a subgroup of that order, which is cyclic and thus has an element of order of that prime, so the group is not a *p*-group. Conversely, suppose that a *p*-group has an element of order of a power of some other prime. Then that would generate a subgroup of other prime power order which would hence not divide the order of the group, which is impossible by Lagrange.

15. $P \lhd N_G P \Rightarrow \quad \forall g \in N_G P : i_g P = P$ so by the Second Sylow Theorem, $N_G P$ has only the *p*-subgroup *P*. Now, suppose $N_G N_G P \supset N_G P \Rightarrow \quad \exists g \in N_G N_G P \setminus N_G P : i_g P \neq P \Rightarrow \quad i_g P \not\subseteq N_G P$, so there is another *p*-subgroup outside of $N_G P$. However, $g \in N_G N_G P \Rightarrow \quad i_g N_G P = N_G P$ and $P \subseteq N_G P \Rightarrow \quad i_g P \subseteq i_g N_G P = N_G P$ so this other *p*-subgroup would have to be inside of $N_G P$. This is a contradiction, so $N_G N_G P \not\supset N_G P$. Therefore $N_G N_G P = N_G P$.

16. By Cauchy, *H* is contained in some maximal *p*-subgroup P' of *G*. By the Second Sylow Theorem, $\exists g \in G : g P' g^{-1} = P \Rightarrow \quad g H g^{-1} \subseteq P$.

17. $\left|G\right| = 35^3 = 5^3 7^3$, so the 5-subgroups in *G* have order $5^3 = 125$. The only divisors of 125 that can be in $5\mathbb{Z}+1$ cannot contain powers of 5, and $\left(5\mathbb{Z}+1\right) \cap \left\{7^0 = 1, 7^1 = 7, 7^2 = 49, 7^3 = 343\right\} = \left\{1\right\}$, so the only 5-subgroup is normal.

18. The only divisors of $\left|G\right|$ that can be in $17\mathbb{Z}+1$ cannot contain powers of 17. The largest remaining divisor of G is $3 \cdot 5 = 15 < 18$ also cannot possibly be in $17\mathbb{Z}+1$. Therefore there is one normal 17-subgroup.

19. The number of *p*-subgroups divides $p^r m$ and is in $p\mathbb{Z}+1$, so the divisors $p^{s \le r} m^{t \le 1}$ cannot contain any powers of *p*. The only possible divisors therefore are $m^{0,1}$, but since $m < p$ it cannot be in $p\mathbb{Z}+1$. So there is one normal *p*-subgroup.

20. a. $G_G = \left\{g \in G \mid \forall x \in G : i_x g = x g x^{-1} = g\right\} = \left\{g \in G \mid \forall x \in G : xg = gx\right\} = \mathrm{Z}G$.

b. By Theorem 1, $\left|G\right| - \left|G_G\right|$ is divisible by *p*, and because *G* is a *p*-group and thus divisible by *p*, so is G_G. Because G is nontrivial, $p > 1$. Since $e \in G_G, \left|G_G\right| > 1$ so $G_G = \mathrm{Z}G$ is nontrivial.

21. By the First Sylow Theorem, we know that a group *G* with the given characteristics has a subnormal series. The Exercise asks us to prove that it has a normal series. We will prove this by showing that any subnormal series is itself a normal series.

Let $\left({}_{0 \le i \le n} H_i\right)$ be a subnormal series of *G*; we show that these are the only subgroups of *G*. Let *H* be a subgroup of *G*. Since *G* is a *p*-group, *H* is a *p*-subgroup and $\exists i : 0 \le i \le n : \left|H\right| = p^i$, so we may reasonably refer to this subgroup as H'_i. By the First Sylow Theorem, this group is contained in an H'_{i+1} and so on. Obviously for some *k*, $H_k = H'_k$. By the First and Second Sylow Theorem, H_{k-1}, H'_{k-1} are normal conjugate maximal *p*-subgroups of H_k, so $H_{k-1} = H'_{k-1}$, and so forth.

Now we show by induction that every $H_i \lhd G$. Obviously $H_0 = E \lhd G$. Consider $\mathrm{Z}G$. By Exercise 20, $\mathrm{Z}G = H_{k_0}$ for some $0 < k_0 \le n$. Now for $\forall i : 0 < i \le k_0 : H_i \subseteq \mathrm{Z}G$ so $\forall h \in H : \forall g \in G : hg = gh \Rightarrow \quad H_i \lhd G$. If $k_0 = n$ we are done. Otherwise, consider G/H_{k_0}, and since $\left|G/H_{k_0}\right| = \left|G\right| / \left|H_{k_0}\right| = p^n / p^{k_0} = p^{n-k_0}$ it is again a *p*-subgroup. The same argument shows that $\mathrm{Z}\left(G/H_{k_0}\right) = H_{k_1} / H_{k_0}$ for some $k_0 < k_1 \le n$. For $\forall i : k_0 < i \le k_1 : H_{k_1} / H_{k_0} \subseteq \mathrm{Z}\left(G/H_{k_0}\right) \quad \Rightarrow \ldots \quad \Rightarrow H_{k_1} / H_{k_0} \lhd G/H_{k_0}$. If $\gamma : G \to G/H_{k_0}$ is the canonical homomorphism, then $\gamma^{\mathrm{inv}} \, H_{k_1} / H_{k_0} = H_{k_1} \lhd G$. Since $k_i > k_{i-1}$, this procedure terminates under induction.

22. Let *H* be a normal *p*-subgroup of *G*, so *H* is invariant under conjugation by *G*. By the First Sylow Theorem, *H* is contained in at least one maximal *p*-subgroup. Since by the Second Sylow Theorem every other maximal *p*-

subgroup is conjugate to this one, and since H is invariant under conjugation, H is also contained in every conjugate.

§4.3 Applications of the Sylow Theory

1. a. The table lists the conjugations $i_g x = gxg^{-1}$:

x	g	ρ_1		ρ_2		ρ_3		μ_1		μ_2		δ_1		δ_2	
	g^{-1}		ρ_3		ρ_2		ρ_1		μ_1		μ_2		δ_1		δ_2
ρ_1		ρ_2	ρ_1	ρ_3	ρ_1	ρ_0	ρ_1	δ_2	ρ_3	δ_1	ρ_3	μ_1	ρ_3	μ_2	ρ_3
ρ_2		ρ_3	ρ_2	ρ_0	ρ_2	ρ_1	ρ_2	μ_2	ρ_2	μ_1	ρ_2	δ_2	ρ_2	δ_1	ρ_2
ρ_3		ρ_0	ρ_3	ρ_1	ρ_3	ρ_2	ρ_3	δ_1	ρ_1	δ_2	ρ_1	μ_2	ρ_1	μ_1	ρ_1
μ_1		δ_1	μ_2	μ_2	μ_1	δ_2	μ_2	ρ_0	μ_1	ρ_2	μ_1	ρ_1	μ_2	ρ_3	μ_2
μ_2		δ_2	μ_1	μ_1	μ_2	δ_1	μ_1	ρ_2	μ_2	ρ_0	μ_2	ρ_3	μ_1	ρ_1	μ_1
δ_1		μ_2	δ_2	δ_2	δ_1	μ_1	δ_2	ρ_3	δ_2	ρ_1	δ_2	ρ_0	δ_1	ρ_2	δ_1
δ_2		μ_1	δ_1	δ_1	δ_2	μ_2	δ_1	ρ_1	δ_1	ρ_3	δ_1	ρ_2	δ_2	ρ_0	δ_2

So the conjugate classes are $\{\rho_0\}, \{\rho_1, \rho_3\}, \{\rho_2\}, \{\mu_1, \mu_2\}, \{\delta_1, \delta_2\}$.

b. $8 = 2 + 2 + 2 + 2$.

2.

	0	1	2	3	4	5	6	7	8	9
00	–	♦	♦	♦	♣	♦	♥	♦	♣	♣
10	♥	♦		♦	♥	♥	♣	♦	♠	♦
20	♠	♥	♥	♦		♣	♥	♣	♠	♦
30	E12	♦	♣	♥	♥	♥	E14	♦	♥	♥
40	N40	♦	♠	♦	♠	N45	♥	♦	E13	♣
50	♠	♥	♠	♦	♣	♥		♥	♥	♦

♦	prime
♣	Example 9
♥	Theorem 7
♠	Exercise 2.19
N40	$40 = 2^3 5$ has one 5-subgroup
N45	$45 = 3^2 5$ has one 5-subgroup

3. a. true ($159 = 53 \cdot 3$, and $53 = 27 \cdot 3 + 2$ so cyclic by Theorem 7)
b. true ($102 = 2 \cdot 3 \cdot 17$, not simple by Exercise 2.19)
c. false (Example 3.4.17 shows S_3 is solvable, and $|S_3| = 3! = 6$)
d. true (Theorem 1)
e. true
f. true (Theorem 7)
g. true ($125 = 5^3$, by Exercise 21 has a normal subgroup of order 5^1, i.e. commutes with every element)
h. true ($42 = 2 \cdot 3 \cdot 7$, by Exercise 2.19)
i. false ($42 = 2 \cdot 3 \cdot 7$ cannot by Lagrange even have any subgroup of that order)
j. false (trivially, A_5 is simple)

4. Let G be a group of order $5 \cdot 7 \cdot 47$. By familiar reasoning, it has one 5-subgroup H_5 and one 7-subgroup H_7. Then $|G / H_5| = 7 \cdot 47$ and $|G / H_7| = 5 \cdot 47$ so both factor groups are cyclic by Theorem 7. Then by Theorem 3.3.20, $H_5, H_7 \supseteq \mathrm{C}G$ contain the commutator subgroup of G, so $|\mathrm{C}G| \in \{1,5\} \cap \{1,7\}$ so $\mathrm{C}G = E$. Therefore $G / \mathrm{C}G = G / E \cong G$ is commutative, and each of its subgroups is normal.

5. Let G be a group of order $96 = 2^5 3$. The number of 2-subgroups of order $2^5 = 32$ must be 1 or 3. Suppose it has 3, and let H and K be two distinct ones. $H \cap K$ is again a 2-subgroup of order a power of 2. If $|H \cap K| = 2^3$ then by Lemma 8 $|HK| = \dfrac{2^5 \cdot 2^5}{2^3} = 2^7 = 128 > 96 = |G|$ which is impossible. Since $H \neq K \Rightarrow \quad |H \cap K| < |G|$, so $|H \cap K| = 2^4$. Then $|H| \big/ |H \cap K| = 2^5 \big/ 2^4 = 2$, so $H \cap K \triangleleft G$.

6. Let G be a group of order $160 = 2^5 5$. The number of 2-subgroups of order $2^5 = 32$ must be 1 or 5. Suppose it has

5, and let H and K be two distinct ones. $H \cap K$ is again a 2-subgroup of order a power of 2. If $\left|H \cap K\right| = 2^2$ then by Lemma 8 $\left|HK\right| = \dfrac{2^5 \cdot 2^5}{2^2} = 2^8 = 256 > 160 = \left|G\right|$ which is impossible. Since $H \neq K \Rightarrow \quad \left|H \cap K\right| < \left|G\right|$, so $\left|H \cap K\right| \in \left\{2^3, 2^4\right\}$. By Exercise 2.21, $H \cap K \lhd H, K \Rightarrow \quad N_G\left(H \cap K\right) \supset H, K$ and (why?) $\left|N_G\left(H \cap K\right)\right| = n \cdot 2^5$, $n > 1$ and divides the order of G, so $\left|N_G\left(H \cap K\right)\right| = \left|G\right| \Rightarrow \quad N_G\left(H \cap K\right) = G$, so $H \cap K \lhd G$.

7. a. $\tau\sigma\tau^{-1} = \tau\left(a_0\ a_2\ \ldots\ a_{m-1}\right)\tau^{-1}$, so the only letters affected by σ are the τa_i and all other letters are invariant under the entire product. $\forall i : \left(\tau\sigma\tau^{-1}\right)\left(\tau a_i\right) = \left(\tau\sigma\tau\tau^{-1}\right)a_i = \left(\tau\sigma\right)a_i = \tau\left(\sigma a_i\right) = \tau a_{(i+1) \bmod m}$, so $\tau\sigma\tau^{-1} = \left(\tau a_0\ \tau a_1\ \ldots\ \tau a_{m-1}\right)$.0

b. For any two cycles of the same length $\alpha = \left(a_0\ a_1\ \ldots\ a_{m-1}\right)$, $\beta = \left(b_0\ b_1\ \ldots\ b_{m-1}\right)$, let $\alpha' = \left(a_0'\ a_1'\ \ldots\ a_{n-1}'\right)$ be any cycle of all the letters not in α, and β similarly. Then define $\tau : \begin{cases} \exists i : x = a_i & x \mapsto b_i \\ \exists i : x = a_i' & x \mapsto b_i' \end{cases}$, which is a bijection and a permutation. By (a.), $\tau\alpha\tau^{-1} = \tau\left({}_i\ a_i\right)\tau^{-1} = \left({}_i\ \tau a_i\right) = \left({}_i\ b_i\right) = \beta$, so $\alpha \sim \beta$.

c. Write the products of cycles as $\alpha = \cdot_{i<s}\alpha_i = \cdot_{i<s}\left({}_{j<r_i}\ a_{ij}\right)$, $\quad \beta = \cdot_{i<s}\beta_i = \cdot_{i<s}\left({}_{j<r_i}\ b_{ij}\right)$, and let $\alpha_s = \left({}_{j<r_s}\ a_j\right)$ be any cycle of all the letters not in any $\alpha_{i<s}$, and β similarly. Then define $\tau : \exists i \leq s, j < r_s : x = a_{ij} \mapsto b_{ij}$, which is a bijection and a permutation. Then $\tau\sigma\tau^{-1} = \tau\left(\cdot_{i\leq s}\ \alpha_i\right)\tau^{-1} \overset{\alpha_i \text{ disjoint}}{=} \left(\cdot_{i\leq s}\ \tau\alpha_i\tau^{-1}\right) \overset{\text{(b.)}}{=} \left(\cdot_{i\leq s}\ \beta_i\right) = \beta$.

d. Differently factored disjoint products cannot be conjugate. Any disjoint factoring into cycles is unique: disjoint factors cannot be combined into a cycle, and a cycle cannot be split into disjoint factors. For any disjoint permutation, every letter must be in exactly one cycle (perhaps a 1-cycle). So pn as described gives the number of ways permutations of S_n are factored into disjoint cycles, which are (by c.) the conjugate classes.

e.

$p1 = 1$	1
$p2 = 2$	1 1, 2
$p3 = 3$	1 1 1, 2 1, 3
$p4 = 5$	1 1 1 1, 1 1 2, 2 2, 3 1, 4
$p5 = 7$	1 1 1 1 1, 1 1 1 2, 1 2 2, 1 1 3, 2 3, 1 4, 5
$p6 = 11$	1 1 1 1 1 1, 1 1 1 1 2, 1 1 2 2, 2 2 2, 1 1 1 3, 1 2 3, 3 3, 1 1 4, 2 4, 1 5, 6
$p7 = 15$	1 1 1 1 1 1 1, 1 1 1 1 1 2, 1 1 1 2 2, 1 2 2 2, 1 1 1 1 3, 1 1 2 3, 2 2 3, 1 3 3, 1 1 1 4, 1 2 4, 3 4, 1 1 5, 2 5, 1 6, 7

8. By Exercise 7, S_4 has 5 conjugate classes:

$\dfrac{4!}{4!} = 1$	(1)(2)(3)(4)
$\dfrac{4!}{2! \cdot 2!} = 6$	(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)
$\dfrac{4!}{2! \cdot 2 \cdot 2} = 3$	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)
$\dfrac{4!}{3} = 8$	(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)
$\dfrac{4!}{4} = 6$	(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)

$24 = 1 + 6 + 3 + 8 + 6$

9. The class equation can be found as follows. First, find the structure of each of the conjugate classes as in Exercise 7e. To find the number of distinct permutations in each conjugate class, imagine listed in a table the $n!$ different ways of writing the letters of S_n, and draw dividing lines between the columns of this table so as to separate each row into cycles according to the partition of the conjugate class. This surely represents every possible element of the class, although each element may be overrepresented. In particular, if the conjugate class has m_l cycles of a certain

length *l*, the m_l! rearrangements of these cycles within a permutation are equivalent. Also, every cycle of length *p* can itself be written in *p* different ways by 'rotating' its letters. So the number of cycles of a conjugate class is $\frac{n!}{\cdot_l m_l! \cdot_i p_i}$. With the help of the partitioning found in Exercise 7,

$$S_5: \qquad 5! = \frac{5!}{5!} + \frac{5!}{3!\cdot 2} + \frac{5!}{2!\cdot 2\cdot 2} + \frac{5!}{2!\cdot 3} + \frac{5!}{2\cdot 3} + \frac{5!}{4} + \frac{5!}{5} \quad \Leftrightarrow \quad 120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$$

$$S_6: \qquad 6! = \frac{6!}{6!} + \frac{6!}{4!\cdot 2} + \frac{6!}{2!\,2!\cdot 2\cdot 2} + \frac{6!}{3!\cdot 2\cdot 2\cdot 2} + \frac{6!}{3!\cdot 3} + \frac{6!}{2\cdot 3} + \frac{6!}{2!\cdot 3\cdot 3} + \frac{6!}{2!\cdot 4} + \frac{6!}{2\cdot 4} + \frac{6!}{5} + \frac{6!}{6} \quad \Leftrightarrow$$
$$720 = 1 + 15 + 45 + 15 + 40 + 120 + 40 + 90 + 90 + 144 + 120$$

10. By Theorem 2.4.12 the commutative groups of order p^n are isomorphic to $\times_i \mathbb{Z}_{p^{n_i}}$, where $\cdot_i p^{n_i} = p^n \Rightarrow \quad +_i n_i = n$. Therefore the commutative groups of order p^n differ only (up to isomorphism) in the distribution of *n*, which can be done in *pn* ways.

11. $\mathrm{Z} S_n = \left\{\sigma \in S_n \mid \forall \tau \in S_n : \sigma\tau = \tau\sigma\right\} = \left\{\sigma \in S_n \mid \sigma = \tau\sigma\tau^{-1}\right\}$, so the center of S_n is the permutations that are invariant under conjugation of all S_n, which is the conjugate classes of S_n that have exactly one element. By Exercise 7 the conjugate class consisting only of 1-cycles contains only the identity. Also, any permutation containing an *n*-cycle will be conjugate to every other permutation with an *n*-cycle. If $n > 2$ two distinct *n*-cycles can always be found, so that the conjugate class has more than one element. Therefore, for $n > 2$ $\mathrm{Z} S_n = E$.

§4.4 Free Abelian Groups

1. $\left\{(1,1,1), (1,2,1), (1,1,2)\right\}$.

2. $\left\langle (2,1), (3,1) \right\rangle = \left\langle (2,1), (1,0) \right\rangle = \left\langle (0,1), (1,0) \right\rangle = \mathbb{Z} \times \mathbb{Z}$

$$\alpha(2,1) + \beta(3,1) = (0,0) \Rightarrow \begin{cases} 2\alpha + 3\beta = 0 \\ 1\alpha + 1\beta = 0 \end{cases} \Rightarrow \begin{cases} 2\alpha + 3(-\alpha) = -\alpha = 0 \\ \beta = -\alpha \end{cases} \Rightarrow \begin{cases} \alpha = 0 \\ \beta = 0 \end{cases}$$

So this does form a basis.

3. $\left\langle (2,1), (4,1) \right\rangle = \left\langle (2,1), (2,0) \right\rangle = \left\langle (0,1), (2,0) \right\rangle \neq \mathbb{Z} \times \mathbb{Z}$ does not form a basis.

4. $\left\{(a,b), (c,d)\right\}$ is a basis for $\mathbb{Z} \times \mathbb{Z}$ iff (Theorem 1, Condition 2) $\left\langle (a,b), (c,d) \right\rangle = \mathbb{Z} \times \mathbb{Z}$ and $\alpha(a,b) + \beta(c,d) = (0,0) \Rightarrow \quad \alpha, \beta = 0$. Show that these conditions are equivalent to being able to generate (1,0) and (0,1).

$\Rightarrow$Suppose that $\exists \alpha_{1,2}, \beta_{1,2} : \begin{cases} \alpha_1(a,b) + \beta_1(c,d) = (1,0) \\ \alpha_2(a,b) + \beta_2(c,d) = (0,1) \end{cases}$. Prove that this implies $\left\{(a,b), (c,d)\right\}$ is a basis by showing that it satisfies Condition 2 of Theorem 1. For any $(e,f) \in \mathbb{Z} \times \mathbb{Z}$,

$$(e,f) = e(1,0) + f(0,1) = e\left(\alpha_1(a,b) + \beta_1(c,d)\right) + f\left(\alpha_2(a,b) + \beta_2(c,d)\right) = \left(e\alpha_1 + f\alpha_2\right)(a,b) + \left(e\beta_1 + f\beta_2\right)(c,d)$$

so $\left\langle (a,b), (c,d) \right\rangle = \mathbb{Z} \times \mathbb{Z}$. Next,

$$\begin{aligned} \alpha(a,b) + \beta(c,d) = (0,0) \quad &\Rightarrow \alpha\left(a(1,0) + b(0,1)\right) + \beta\left(c(1,0) + d(0,1)\right) = (0,0) \\ &\Rightarrow \left(\alpha a + \beta c\right)(1,0) + \left(\alpha b + \beta d\right)(0,1) = (0,0) \\ &\Rightarrow \alpha a + \beta c = 0 \wedge \alpha b + \beta d = 0 \\ &\Rightarrow \left(\alpha = 0 \vee a = 0\right) \wedge \left(\beta = 0 \vee c = 0\right) \wedge \left(\alpha = 0 \vee b = 0\right) \wedge \left(\beta = 0 \vee d = 0\right) \end{aligned}$$

Suppose $\alpha \neq 0$, then $a = 0$ and $b = 0$, but then $\left\{(a,b), (c,d)\right\}$ cannot possibly generate $\mathbb{Z} \times \mathbb{Z}$. Similarly $\beta \neq 0$ is impossible. So $\alpha, \beta = 0$.

$\Leftarrow$If $\left\{(a,b), (c,d)\right\}$ is a basis, then obviously they can generate (1,0) and (0,1).

Now, find conditions on *a*, *b*, *c*, *d* such that $\exists \alpha_{1,2}, \beta_{1,2} : \begin{cases} \alpha_1(a,b) + \beta_1(c,d) = (1,0) \\ \alpha_2(a,b) + \beta_2(c,d) = (0,1) \end{cases}$, that is

$$\begin{cases}\alpha_1 a+\beta_1 c=1\\ \alpha_1 b+\beta_1 d=0\end{cases} \wedge \begin{cases}\alpha_2 a+\beta_2 c=0\\ \alpha_2 b+\beta_2 d=1\end{cases}.$$

- First, suppose $a=0$. Then $\begin{cases}[1]\ \ \beta_1 c=1\Rightarrow\beta_1,c=\pm1\\ [4]\ \ \pm\alpha_1\pm d=0\Rightarrow d=\pm\alpha_1\end{cases} \wedge \begin{cases}[2]\ \ \beta_2 c=0\Rightarrow\beta_2=0\\ [3]\ \ \alpha_2 b=1\Rightarrow b=\pm1\end{cases}$, so $\left\{(0,\pm1),\ (\pm1,d)\right\}$ are possible bases. Similarly for b, c, or $d = 0$.
- The remainder of the cases have $a,b,c,d\neq0$. Then

$$\begin{cases}[2]\ \left(-\beta_1\cdot d/b\right)a+\beta_1 c=1\Rightarrow\quad\left(-ad/b+c\right)\beta_1=1\\ [1]\ \ \alpha_1 b=-\beta_1 d\Rightarrow\quad\alpha_1=-\beta_1\cdot d/b\end{cases}\wedge\begin{cases}\ldots\\ \ldots\end{cases}\Rightarrow\begin{cases}-ad/b+c\neq0\\ \end{cases}\wedge\begin{cases}\\ b-ad/c\neq0\end{cases}\Rightarrow ad\neq bc$$

This is the familiar condition of linear independence that the determinant formed by a basis be nonzero.

5. Replace "generating set" with "basis."

6. Correct.

7. $2\mathbb{Z}\subset\mathbb{Z}$ both have rank 1.

8. a. true (Exercise 10)
 b. true (any minimal generating set is a basis)
 c. true ($\mathbb{Z}^n$)
 d. true (the condition implies that the group is torsion-free)
 e. true
 f. false (if $\Upsilon\supset X$ the expression of elements in terms of Υ is not unique)
 g. false ($\mathbb{Z}$ has only $\left\{\pm1\right\}$ as bases)
 h. true (Theorem 9)
 i. true (why?)
 j. false ($\mathbb{Z}/2\mathbb{Z}=\mathbb{Z}_2$ is not free commutative)

9.
- (injective) $\exists g,g'\in G:\phi g=\phi g',\quad\exists n_i,n_i':g=+_i\ n_i x_i,\ g'=+_i\ n_i' x_i\Rightarrow\quad\left({}_i\ n_i\right)=\left({}_i\ n_i'\right)\Rightarrow\quad g=g'$.
- (surjective) $\forall\left({}_i\ n_i\right)\in\mathbb{Z}^r:\exists g\in G:g=+_i\ n_i x_i,\ \phi g=\left({}_i\ n_i\right)$.
- (associative) For all $\forall g,g'\in G:\exists n_i,n_i':g=+_i\ n_i x_i,\ g'=+_i\ n_i' x_i$,

$$\phi g+\phi g'=\phi\left({}_i\ n_i x_i\right)+\phi\left({}_i\ n_i' x_i\right)=\left({}_i\ n_i\right)+\left({}_i\ n_i'\right)=\left({}_i\ n_i+n_i'\right)=\phi\left({}_i\ \left(n_i+n_i'\right)x_i\right)=\phi\left(\left({}_i\ n_i x_i\right)+\left({}_i\ n_i' x_i\right)\right)=\phi\left(g+g'\right).$$

10. If G had an element $g\in G$ of order n, and $g=+_i\ \alpha_i x_i$ for some basis $\left\{{}_i\ x_i\right\}$, then $g=ng+g=\left(n+1\right)g=\left(n+1\right)\left(+_i\ \alpha_i x_i\right)=+_i\ \left((n+1)\alpha_i\right)x_i$, contradicting the uniqueness of the expression of g in terms of its basis elements.

11. Let X and X' be bases for G and G', respectively. Show that Condition 2 of Theorem 1 holds:
- $\forall\left(g,g'\right)\in G\times G':g\in G,g'\in G'\Rightarrow\quad\exists n_i,n_i':g=+_i\ n_i x_i,\ g'=+_i\ n_i' x_i'\Rightarrow\quad\left(g,g'\right)=\left(+_i\ n_i x_i,+_i\ n_i' x_i'\right)$ so $\left\langle\cup_i\ \left(x_i,0\right)\cup_i\ \left(0,x_i'\right)\right\rangle=G\times G'$.
- $\left(+_i\ n_i x_i,+_i\ n_i' x_i'\right)=(0,0)\Rightarrow\quad+_i\ n_i x_i=0\wedge+_i\ n_i' x_i'=0\Rightarrow\quad n_i=0\wedge n_i'=0$.

12. ⇒ If G is free commutative of finite rank, then by Condition 2 of Theorem 1 the finite basis generates it. By Exercise 10 it has no elements of finite order.

 ⇐ Let X be a minimal generating set of G. We just have to prove 'the uniqueness of zero'. Suppose $+_i\ n_i x_i=0$, and let K partition the coefficients such that $n_{k\in K}\neq0,n_{k\notin K}=0$, and $+_{i\in K}\ n_i x_i=0$. Suppose there is $\exists k\in K$, and thus $n_k x_k=+_{i\in K,i\neq k}\ n_i x_i$. If $+_{i\in K,i\neq k}\ n_i x_i\neq0$ then it and $n_k x_k$ are different expressions of the same element so X could not have been minimal. If $+_{i\in K,i\neq k}\ n_i x_i=0$ then x_k is an element of finite order n_k. So $K=\varnothing$.

13. Since for any prime p, $1/p^n$ cannot be formed from $1/q^m$ for any other prime q, or from $1/p^{n'}$ for $n'<n$, a basis for $\mathbb{Q}$ would have to contain at least $\left\{{}_{p\in\mathbb{P}}\ \lim_{n\to\infty}p^{-n}\right\}$, but no element can have a definite expression in terms of such a basis.

14. Clearly the torsion subgroup is finite. By the First Sylow Theorem, T has a p-subgroup T_p of elements of some power of p, and p does not divide $\left|T/T_p\right|$. So T/T_p has no elements of order p, which must therefore all be in T_p.

15. Since T is isomorphic to its prime-power decomposition, the subgroup T_p of all elements of power of p has a corresponding subgroup of all elements of power of p in the decomposition, which is exactly the direct product of the cyclic factors of order some power of p.

16. $G[n] \subseteq G$ follows from:
- (identity) $0 \in G : n0 = 0 \quad \Rightarrow 0 \in G[n]$;
- (inverse) $\forall g \in G[n] : ng = 0 \quad \Rightarrow \left(ng\right)^{-1} = 0 \quad \overset{\text{commutative}}{\Rightarrow} \quad n\left(g^{-1}\right) = 0 \quad \Rightarrow g^{-1} \in G[n]$;
- (closure) $\forall g, g' \in G[n] : ng = 0, ng' = 0 \quad \Rightarrow \left(ng\right)\left(ng'\right) \overset{\text{commutative}}{=} n\left(gg'\right) = 0 \quad \Rightarrow gg' \in G[n]$.

17. $g \in \mathbb{Z}_{p^r}[p] \quad \Leftrightarrow pg = 0 \quad \Leftrightarrow \exists n : pg = n \cdot p^r \quad \Leftrightarrow g = np^{r-1} \quad \Rightarrow \left|\mathbb{Z}_{p^r}[p]\right| = p$, and $\mathbb{Z}_{p^r}[p] \subseteq \mathbb{Z}_{p^r}$ is commutative, so $\mathbb{Z}_{p^r}[p] \cong \mathbb{Z}_p$.

18. $\left(\times_i \mathbb{Z}_{p^i}\right)[p] = \times_i \mathbb{Z}_{p^i}[p] \cong \times_i \mathbb{Z}_p$.

19. a. If $\times_i \mathbb{Z}_{p^{r_i}} \cong \times_i \mathbb{Z}_{p^{s_i}} \quad \Rightarrow \left(\times_i \mathbb{Z}_{p^{r_i}}\right)[p] \cong \left(\times_i \mathbb{Z}_{p^{s_i}}\right)[p] \quad \Rightarrow \times_i \mathbb{Z}_{p^{r_i}} \cong \times_i \mathbb{Z}_{p^{s_i}} \quad \Rightarrow \mathbb{Z}_{p^m} \cong \mathbb{Z}_{p^n} \quad \Rightarrow m = n$.

    b. Let $j \geq 0$ such that $\forall i < j : r_i = s_i; r_j < s_j$. Certainly $p^{r_j} \cdot \times_i \mathbb{Z}_{p^{r_i}} \cong p^{r_j} \cdot \times_i \mathbb{Z}_{p^{s_i}} \Rightarrow \times_i p^{r_j} \mathbb{Z}_{p^{r_i}} \cong \times_i p^{r_j} \mathbb{Z}_{p^{s_i}}$. Now, for any $q \leq r_j$, $p^{r_j} \mathbb{Z}_{p^q} = E$, so $\times_{i<j} E \quad \times_{i=j} E \quad \times_{i>j} p^{r_j} \mathbb{Z}_{p^{r_i}} \cong \times_{i<j} E \quad \times_{i=j} p^{r_j} \mathbb{Z}_{p^{s_i}} \quad \times_{i>j} p^{r_j} \mathbb{Z}_{p^{s_i}}$ with $p^{r_j} \mathbb{Z}_{p^{s_j}} \neq E \quad \Leftarrow r_j < s_j$, but this is impossible by (a).

20. Factorize each of the torsion coefficients $m_i = \cdot_j \, p_j^{q_j}, \quad p_j \in \mathbb{P}, q_j \in \mathbb{N}^+$, then $G = \times_i \times_j \mathbb{Z}_{p_j^{q_j}}$. For example, $T = \mathbb{Z}_{216} \times \mathbb{Z}_4 \quad \Rightarrow m_0 = 2^3 3^3, m_1 = 2^2 \quad \Rightarrow G = \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{2^2}$.

21. From Exercise 2.4.42, $m_j = \cdot_{i:j<n_i} \, p_i^{q_{ij}} \quad \Rightarrow m_0 = \cdot_i \, p_i^{q_{i0}}$ where q_{i0} is the highest power of p_i in the decomposition.

22. From Exercise 2.4.42 (not really proved there).

§4.5 Free Groups

1. a. $a^2 b^2 a^3 c^3 b^{-2}$; $b^2 c^{-3} a^{-3} b^{-2} a^{-2}$; b. $a^{-1} b^3 a^4 c^6 a^{-1}$; $a^1 c^{-6} a^{-4} b^{-3} a^1$.

2. a. $a^5 c^3$; $a^{-5} c^{-3}$; b. $a^{-4} b^{-3} c^{-6}$; $a^4 b^3 c^6$.

3. By Theorem 12, there is exactly one homomorphism for each selection of 2 elements in the range G', so there are $\left|G'\right|^2$ homomorphisms: a. $\left|G\right|^2 = 4^2 = 16$; b. $\left|G\right|^2 = 6^2 = 36$; c. $\left|G\right|^2 = 3!^2 = 6^2 = 36$.

4. In this case, the ϕa_i must also generate G'. a. $\left(2 \cdot \left(2 \cdot 4\right) - 2^2\right) = 12$; b. $\left(2 \cdot \left(2 \cdot 6\right) - 2^2\right) + 2 \cdot \left(2 \cdot 1\right) = 20 + 4 = 24$; c. $2 \cdot \left(2 \cdot 3\right) + 2 \cdot \left(3 \cdot 2\right) = 24$.

5.

6.

7. Correct.

8. Insert “free” before “generators”. I don't think it's been proved that there are no other generators.

9. “It would seem obvious that this operation of multiplication is well-defined and associative.” I think this is obvious too. Can't think of anything that might throw a spoke in the wheel.

10. a. false (E is not free by definition)

    b. false (a subgroup of a commutative group is commutative and thus not generally free)

    c. false (the image of the trivial homomorphism is not free)

    d. true (by Definition 4.2)

e. false (torsion groups are finitely generated but not free commutative)
f. false (is this a trick question?)
g. false (a free group generated by one element is free commutative on the basis of that element)
h. true (a free commutative group of rank greater than one must have more than one generator, but any free group with more than one generator is not commutative)
i. false (Theorem 9)
j. true (Theorem 4.5)

11. a. $1\cdot 2+2\cdot 3=0, \quad 1\cdot 2=1, 2\cdot 3=2$. $\{1\}$ is a basis for $\mathbb{Z}_4$, certainly $\langle 1\rangle=\mathbb{Z}_4$ and any one-element generating set is a basis under the definition.

b. $\{1\}$ is a one-element generating set and hence a basis. Also, $\langle\{2,3\}\rangle=\mathbb{Z}_6$.
$+_i\, m_i b_i=0 \quad \Rightarrow m_0\cdot 2+m_1\cdot 3=0 \quad \Rightarrow 2m_0=-3m_1$ so m_0 is a multiple of 3 and m_1 is a multiple of 2, so $2m_0$ and $3m_1$ are multiples of 6, so $2m_0=0, \quad 3m_1=0$.

c. No, because a basis of a free commutative group induces unique expressions in terms of it.

d. A finite commutative group has an expression in terms of torsion coefficients, one dividing the next, where each factor in the direct product has an element of the order of its coefficient.

12. a.

$$\begin{tikzcd}
G \arrow[rr, "\phi_2=\theta_2\phi_1"] \arrow[dr, bend right, "\phi_1"'] & & G_2^* \\
& G_1^* \arrow[ur, bend right, "\theta_2"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[rr, "\phi_1=\theta_1\phi_2"] \arrow[dr, bend right, "\phi_2"'] & & G_1^* \\
& G_2^* \arrow[ur, bend right, "\theta_1"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[rr, "\psi"] \arrow[d] \arrow[dr] & & G' \\
G/K \arrow[r] & G/\mathrm{Ker}\,\psi \arrow[ur, "\text{isomorphism}"'] &
\end{tikzcd}$$

G_1^*, G_2^* can each be factored in terms of the other, so $\phi_1=\theta_1\phi_2, \phi_2=\theta_2\phi_1$. Then
$\phi_1=\theta_1\phi_2=\theta_1\theta_2\phi_1 \Rightarrow i=\theta_1\theta_2; \quad \phi_2=\theta_2\phi_1=\theta_2\theta_1\phi_2 \Rightarrow i=\theta_2\theta_1$. Now

$$\ker\theta_1=\left\{g\in G_2^* \mid \theta_1 g=e \Rightarrow \theta_2\theta_1 g=e \Rightarrow ig=e\right\}=E; \quad \forall g\in G_1^*: \theta_2 g\in G_2^*: \theta_1(\theta_2 g)=(\theta_1\theta_2)g=ig=g$$

so θ_1 is injective and surjective, so is an isomorphism, so $G_1^*\cong G_2^*$.

b. Consider all possible homomorphisms of G into commutative G', and let K be a minimal set contained by the kernels of all these homomorphisms. If $K_{1,2}\triangleleft G$ are kernels of two homomorphisms such that $G/K_{1,2}$ are commutative, then $K_1\cap K_2\triangleleft G$ must be the kernel of a homomorphism with $G/K_1\cap K_2$ commutative, so K is *the* minimal kernel of all commutative homomorphisms.
Refer to the figure on the right. By Fundamental Homomorphism Theorem, any homomorphism ψ can be factored into a homomorphism onto its kernel factor group and an isomorphism from this group. By Exercise 3.3.35. $K\triangleleft G \Rightarrow \ker\psi\cap K=K\triangleleft \mathrm{K}\ker\psi$, so there are canonical homomorphisms $G\to G/K$ and $G/K\to G/\ker\psi$. G/K is thus a blip group.

c. The blip group of G is its commutator subgroup.

13. a.

$$\begin{tikzcd}
S \arrow[rr, "f'"] \arrow[dr, bend right, "f"'] & & G' \\
& G \arrow[ur, bend right, "\phi_{f'}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
S \arrow[rr, "f_2=\phi_{f_2}f_1"] \arrow[dr, bend right, "f_1"'] & & G_2 \\
& G_1 \arrow[ur, bend right, "\phi_{f_2}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
S \arrow[rr, "f_1=\phi_{f_1}f_2"] \arrow[dr, bend right, "f_2"'] & & G_1 \\
& G_2 \arrow[ur, bend right, "\phi_{f_1}"'] &
\end{tikzcd}$$

Refer to the figure on the left for the adjusted naming. Suppose f is not injective. Then $\exists s_1, s_2\in S, s_1\neq s_2: fs_1=fs_2$. Then there is a group G' and $f': S\to G'$ such that $g_1'=f's_1, g_2'=f's_2$ and $g_1'\neq g_2'$. But then there cannot be a homomorphism $\phi_{f'}$ such that $f'=\phi_{f'}f$, because then
$f's_1=\phi_{f'}fs_1 \Rightarrow \phi_{f'}g_1=g_1'; \quad f's_2=\phi_{f'}fs_2 \Rightarrow \phi_{f'}g_2=\phi_{f'}g_1=g_2'$ and $\phi_{f'}$ would not even be a function.
Now, suppose fS does not generate G. Then there is a $g\in G$ that is not generated by fS, and then for any G', f' and $\phi_{f'}: f'=\phi_{f'}f$ we can let $\phi_{f'}g$ equal any element of G' without affecting $\phi_{f'}f$, contradicting the uniqueness of $\phi_{f'}$.

Now let $G_{1,2}$ be blop groups. The figures on the right illustrate how $f_{1,2}$ can each be factored in terms of the other, so $f_1 = \phi_{f_1} f_2$, $f_2 = \phi_{f_2} f_1$. Then $f_1 = \phi_{f_1}\phi_{f_2} f_1 \Rightarrow \phi_{f_1}\phi_{f_2} = i$; $f_2 = \phi_{f_2}\phi_{f_1} f_2 \Rightarrow \phi_{f_2}\phi_{f_1} = i$. Then
$\ker\phi_{f_1} = \left\{g_2 \in G_2 \mid \phi_{f_1} g_2 = e \quad \Rightarrow \phi_{f_2}\phi_{f_1} g_2 = \phi_{f_2} e \quad \Rightarrow ig_2 = e \quad \Rightarrow g_2 = e\right\} = E$;
$\forall g_1 \in G_1 : \exists g_2 \in G_2 : \phi_{f_1} g_2 = g_1 \quad \Rightarrow \phi_{f_2}\phi_{f_1} g_2 = \phi_{f_2} g_1 \quad \Rightarrow ig_2 = \phi_{f_2} g_1 \quad \Rightarrow g_2 = \phi_{f_2} g_1$,
so ϕ_{f_1} is an isomorphism and $G_1 \cong G_2$.

b. Let $F[S]$ be the free group on $S = \left\{_i\ s_i\right\}$. Then by Theorem 12, for any group G' and $f' : S \to G'$ there is a unique homomorphism $\phi_{f'}$ such that $\phi_{f'} fs_i = f' s_i$ Since $\langle fS \rangle = G$, it follows that $\phi_{f'} f = f'$, so $F[S]$ is a blop group on *S*.

c. A blop group on *S* is the free group on *S*.

14. A group *G* is a free commutative group if it is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{N}^+$.

§4.6 Group Presentations

1. • $\mathbb{Z}_4 \cong \left(a : a^4\right)$

   • Trivially, $\mathbb{Z}_4 \cong \left(a, b : a^4, b\right)$ is akin to saying that *b* does not generate anything at all. Also $\mathbb{Z}_4 \cong \left(a, b : a^4, a^2 b^{-1}\right)$ which implies $a = 1, b = a^2 = 2$.

   • Trivially, $\mathbb{Z}_4 \cong \left(a, b, c : a^4, b, c\right)$. Also, $\mathbb{Z}_4 \cong \left(a, b, c : a^4, a^2 b^{-1}, ac\right)$ implies $a = 1, b = 2, c = a^{-1} = 3$.

2. $S_3 \overset{?}{\cong} \left(\rho_1, \mu_1, \mu_2 : \rho_1^{\ 3}, \mu_1^{\ 2}, \mu_2^{\ 2}, \mu_1 \mu_2 \rho_1^{\ -1}\right)$.

3.

1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	1	a	a^2	a^3b	b	ab	a^2b
b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^2b	ab	b	a^3	a^2	a	1

1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	1	a	a^2	a^3b	b	ab	a^2b
b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^2b	ab	b	a	1	a^3	a^2

4. The commutative groups of order 14 are isomorphic to $\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$. Suppose *G* is a noncommutative group of order 14. Then *G* contains normal subgroups $G_{2,7}$ of order 2 and 7 respectively, and both cyclic so $a \in G : \langle a \rangle = G_2, a^2 = 1$; $b \in G : \langle b \rangle = G_7, b^7 = 1$. Since $G_7 \lhd G$, i_a is an automorphism of G_7 so $i_a b$ must also be an element of order 7, so $i_a b = aba^{-1} \in \left\{_{2 \le i \le 6}\ b^i\right\}$. $i = 1$ is not possible, because this would imply $aba^{-1} = b^1 \Rightarrow ab = ba$ that *G* was commutative. By Exercise 13b. this gives a group of order 14 iff $i^2 =_7 1 \Rightarrow i = 6$. So this leaves $\left(a, b : a^2, b^7, aba^{-1}b^{-6}\right)$.

5. The commutative groups of order 21 are isomorphic to $\mathbb{Z}_{21} \cong \mathbb{Z}_3 \times \mathbb{Z}_7$. Suppose *G* is a noncommutative group of order 21. Then *G* contains normal subgroups $G_{3,7}$ of order 3 and 7 respectively, and both cyclic so $a \in G : \langle a \rangle = G_3, a^3 = 1$; $b \in G : \langle b \rangle = G_7, b^7 = 1$. Since $G_7 \lhd G$, i_a is an automorphism of G_7 so $i_a b$ must also be an element of order 7, so $i_a b = aba^{-1} \in \left\{_{2 \le i \le 6}\ b^i\right\}$. $i = 1$ is not possible, because this would imply $aba^{-1} = b^1 \Rightarrow ab = ba$ that *G* was commutative. By Exercise 13b. this gives a group of order 21 iff $i^3 =_7 1 \Rightarrow i \in \left\{2, 4\right\}$. Why are these isomorphic?

6. "Raised to powers" is redundant.

7. This appears to be completely incorrect. Example 3 shows that presentations with different numbers of generators (between which hence no one-to-one correspondence can exist) can still give isomorphic groups. Rewrite the definition as: “Group presentations are isomorphic iff they give isomorphic groups.”

8. a. true (remark before Example 4; by Theorem 5.13 every group is homomorphic to a free group, and the generators of the kernel are the relators of its presentation)

b. false (depends how you define “different”; E has only $\left(a : a = 1\right)$)

c. false (if the presentations are not isomorphic then neither are the groups)

d. false (the question is unsolvable by the remark after Example 3)

e. false ($\left(a :\right) \cong \mathbb{Z}$ has a finite presentation)

f. true (every cyclic group is isomorphic to $\mathbb{Z}_n \cong \left(a : a^n\right)$)

g. true (the relators form a normal subgroup that is thus invariant under conjugation)

h. false ($\left(a : a^2\right) \cong \mathbb{Z}_2, \left(a : a^3\right) \cong \mathbb{Z}_3$)

i. true ($F[A]/R$ is isomorphic to the group and thus commutative, so R contains the commutator subgroup)

j. true (I think so…)

9. A noncommutative group G of order 15 would have normal subgroups $G_{3,5}$ of order 3 and 5 respectively, and both cyclic so $a \in G : \langle a \rangle = G_3, a^3 = 1$; $b \in G : \langle b \rangle = G_5, b^5 = 1$. Since $G_5 \lhd G$, i_a is an automorphism of G_7 so $i_a b$ must also be an element of order 5, so $i_a b = aba^{-1} \in \left\{_{2 \le i \le 4}\; b^i\right\}$. By Exercise 13b. this gives a group of order 15 iff $i^2 =_5 1$, but this is not so for any i.

10. By Exercise 13b, $\left(a, b : a^3, b^2, ba = a^2 b\right)$ has $2^2 = 4 =_3 1$ so is a group of order $2 \cdot 3 = 6$. If this group were commutative, then $ab = ba \Rightarrow ab = a^2 b \Rightarrow 1 = a$, but then the group would have one generator of order 1 and one of order 2, which cannot possibly generate a group of order 6.

11. By familiar reasoning, $aba^{-1} \in \left\{_{2 \le i \le 2}\; b^i\right\}$ and from Exercise 10 we know $i = 2$ yields S_3. So this must be the only noncommutative group of order 6.

12. A_4 consists of the even permutations on 4 letters, so disjoint products of 1×1×1×1-cycles (order 1), 2×2-cycles (order 2), and 3×1-cycles (order 3), and no elements of order 6, so cannot be isomorphic to $\mathbb{Z}_6$.

S_3 has two elements ($\rho_{1,2}$) of order 3 and three elements ($\mu_{1,2,3}$) of order 2. Suppose A_4 has two elements of order 3, that is two 3-cycles. To form a group, these elements have to be each other's inverse. Without loss of generality, let (1 2 3), (1 3 2) be these two elements. A_4 would have to contain three elements of order 2, that is all three 2×2-cycles. But then $(1\ 2)(3\ 4) \cdot (1\ 2\ 3) = (2\ 4\ 3)$ and A_4 would have to contain at least three elements of order 3, so cannot be isomorphic to S_3 either.

13.

14.

§5.1 Rings and Fields

1. $12 \cdot_{\mathbb{Z}_{24}} 16 = 192 \bmod 24 = 0$.

2. $16 \cdot_{\mathbb{Z}_{32}} 3 = 48 \bmod 32 = 16$.

3. $11 \cdot_{\mathbb{Z}_{15}} -4 = -44 \bmod 15 = 1$.

4. $20 \cdot_{\mathbb{Z}_{26}} -8 = -160 \bmod 26 = 22$.

5. $(2,3) \cdot_{\mathbb{Z}_5 \times \mathbb{Z}_9} (3,5) = (2 \cdot_{\mathbb{Z}_5} 3, 3 \cdot_{\mathbb{Z}_9} 5) = (6 \bmod 5, 15 \bmod 9) = (1,6)$.

6. $(-3,5) \cdot_{\mathbb{Z}_4 \times \mathbb{Z}_{11}} (2,-4) = (-3 \cdot_{\mathbb{Z}_4} 2, 5 \cdot_{\mathbb{Z}_{11}} -4) = (-6 \bmod 4, -20 \bmod 11) = (2,2)$.

7. $n\mathbb{Z}$ are commutative groups. Check multiplication:

- (closed) $\forall na, nb \in n\mathbb{Z} : na \cdot nb = n^2 ab \in n\mathbb{Z}$
- (associative) $\forall na, nb, nc \in n\mathbb{Z} : \left(na \cdot nb\right) \cdot nc = n^2 ab \cdot nc = n^3 abc = na \cdot n^2 bc = na \cdot \left(nb \cdot nc\right)$
- (commutative) $\forall na, nb \in n\mathbb{Z} : na \cdot nb = n^2 ab = n^2 ba = nb \cdot na$

  So they are also commutative fields. Do they have a multiplicative identity?
- (multiplicative identity) $\exists na \in n\mathbb{Z} : \forall nb \in n\mathbb{Z} : na \cdot nb = nb \quad \Rightarrow n^2 ab = nb \quad \Rightarrow na = 1 \quad \Rightarrow n = 1, a = 1$

  So only $1\mathbb{Z} = \mathbb{Z}$ has unity. Which elements have a multiplicative inverse?
- (multiplicative inverse) $\forall a \in \mathbb{Z} : \exists b \in \mathbb{Z} : ab = 1 \quad \Rightarrow a = \pm 1, b = a$

  So not even $\mathbb{Z}$ is a division ring.

8. $\mathbb{Z}^+$ under addition is not even a group.
9. $\mathbb{Z} \times \mathbb{Z}$ is a commutative group. Checking the multiplication:

- (closed) $\forall \left(a_0, a_1\right), \left(b_0, b_1\right) \in \mathbb{Z} \times \mathbb{Z} : \quad \left(a_0, a_1\right) \cdot \left(b_0, b_1\right) = \left(a_0 b_0, a_1 b_1\right) \in \mathbb{Z} \times \mathbb{Z}$
- (associative) $\forall \left(a_0, a_1\right), \left(b_0, b_1\right), \left(c_0, c_1\right) \in \mathbb{Z} \times \mathbb{Z} :$

  $$\left(\left(a_0, a_1\right) \cdot \left(b_0, b_1\right)\right) \cdot \left(c_0, c_1\right) = \left(a_0 b_0, a_1 b_1\right) \cdot \left(c_0, c_1\right) = \left(a_0 b_0 c_0, a_1 b_1 c_1\right) = \left(a_0, a_1\right) \cdot \left(b_0 c_0, b_1 c_1\right) = \left(a_0, a_1\right) \cdot \left(\left(b_0, b_1\right) \cdot \left(c_0, c_1\right)\right)$$
- (commutative) $\forall \left(a_0, a_1\right), \left(b_0, b_1\right) \in \mathbb{Z} \times \mathbb{Z} : \quad \left(a_0, a_1\right) \cdot \left(b_0, b_1\right) = \left(a_0 b_0, a_1 b_1\right) = \left(b_0 a_0, b_1 a_1\right) = \left(b_0, b_1\right) \cdot \left(a_0, a_1\right)$
- (identity) $\exists \left(a_0, a_1\right) \in \mathbb{Z} \times \mathbb{Z} : \forall \left(b_0, b_1\right) \in \mathbb{Z} \times \mathbb{Z} :$

  $$\left(a_0, a_1\right) \cdot \left(b_0, b_1\right) = \left(b_0, b_1\right) \quad \Rightarrow \left(a_0 b_0, a_1 b_1\right) = \left(b_0, b_1\right) \quad \Rightarrow \begin{cases} a_0 b_0 = b_0 \\ a_1 b_1 = b_1 \end{cases} \quad \Rightarrow \begin{cases} a_0 = 1 \\ a_1 = 1 \end{cases}$$
- (inverse) $\forall \left(a_0, a_1\right) \in \mathbb{Z} \times \mathbb{Z} : \exists \left(b_0, b_1\right) \in \mathbb{Z} \times \mathbb{Z} : \quad \left(a_0, a_1\right) \cdot \left(b_0, b_1\right) = (1,1) \quad \Rightarrow \left(a_0 b_0, a_1 b_1\right) = (1,1) \quad \Rightarrow \left(a_0, a_1\right) = (\pm 1, \pm 1)$

  So it is a commutative ring with unity, but not a division ring.

10. $2\mathbb{Z} \times \mathbb{Z}$ is a commutative group. $2\mathbb{Z}, \mathbb{Z}$ are both commutative rings by Exercise 7, so $2\mathbb{Z} \times \mathbb{Z}$ is a commutative ring by Example 7. $2\mathbb{Z}$ does not have a unity by Exercise 7, so neither does $2\mathbb{Z} \times \mathbb{Z}$.
11. $G = \left\{a_0 + a_1\sqrt{2} \mid a_{0,1} \in \mathbb{Z}\right\}$. It is obvious that $X = \left\{1, \sqrt{2}\right\}$ is a generating set for *G*. Now

$$\exists g \in G, g = \left(a + b\sqrt{2}\right), a, b \in \mathbb{Z} : g = 0 \quad \Rightarrow a + b\sqrt{2} = 0 \quad \Rightarrow a, b = 0$$

since there is no common multiple of 1 and $\sqrt{2}$, so *G* is free commutative on *X*. Check multiplication:

- (closed) $\forall \left(a_0 + a_1\sqrt{2}\right), \left(b_0 + b_1\sqrt{2}\right) \in G :$

  $$\left(a_0 + a_1\sqrt{2}\right) \cdot \left(b_0 + b_1\sqrt{2}\right) = a_0 b_0 + \left(a_0 b_1 + a_1 b_0\right)\sqrt{2} + 2a_1 b_1 = \left(a_0 b_0 + 2a_1 b_1\right) + \left(a_0 b_1 + a_1 b_0\right)\sqrt{2} \in G$$

  Multiplicative associativity and commutativity follows from the operation in $\mathbb{R}$. Since $\mathbb{R}$ is a commutative group under addition, *G* is a commutative ring. Obviously $1_G = 1_{\mathbb{R}}$ is the multiplicative identity.
- (inverse) $\forall a = \left(a_0, a_1\sqrt{2}\right) \in G^* : \exists b = \left(b_0, b_1\sqrt{2}\right) \in G^* :$

  $$ab = 1 \quad \Rightarrow \left(a_0, a_1\sqrt{2}\right) \cdot \left(b_0, b_1\sqrt{2}\right) = \left(a_0 b_0 + 2a_1 b_1\right) + \left(a_0 b_1 + a_1 b_0\right)\sqrt{2} = 1 \quad \Rightarrow \begin{cases} a_0 b_0 + 2a_1 b_1 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \end{cases}$$

  From the first equation, $a_0 b_0$ must be odd, but if a_0 is even this is not possible, so *G* is not a division ring.

12. From Exercise 11, *G* is a commutative ring with multiplicative inverse. Also from that exercise,

- (inverse) $\forall a = \left(a_0, a_1\sqrt{2}\right) \in G^* : \exists b = \left(b_0, b_1\sqrt{2}\right) \in G^* :$

  $$\begin{cases} a_0 b_0 + 2a_1 b_1 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \end{cases} \overset{a_0 \neq 0}{\Rightarrow} \begin{cases} a_0 b_0 + 2a_1\left(-a_1 b_0 / a_0\right) = 1 \\ b_1 = -a_1 b_0 / a_0 \end{cases} \quad \Rightarrow \begin{cases} \left(a_0 - 2a_1^{\,2} / a_0\right) b_0 = 1 \\ \ldots \end{cases} \quad \Rightarrow \begin{cases} b_0 = \left(a_0 - 2a_1^{\,2} / a_0\right)^{-1} \\ b_1 = -a_1 b_0 / a_0 \end{cases}$$

  So *a* has inverse *b* if $a_0 \neq 0 \wedge a_0 - 2a_1^{\,2} / a_0 \neq 0 \quad \Rightarrow a_0 = 2a_1^{\,2} / a_0 \quad \Rightarrow 2a_1^{\,2} \neq a_0^{\,2} \quad \Rightarrow a_1 \neq 0$, that is, for all *G**, so *G* is a field.

13. $G = \{ri \mid r \in \mathbb{R}\}$ is not closed under multiplication because $i \cdot i = -1 \in G$, so G is not a ring.

14. The identity of $\mathbb{Z}^*$ is 1. $\forall a \in \mathbb{Z} : \exists b \in \mathbb{Z} : ab = 1 \Rightarrow a = \pm 1$.

15. From Exercise 9, $(\pm 1, \pm 1)$ have inverses.

16. From Example 17, $\{1,2,3,4\} = \mathbb{Z}_5{}^*$ have inverses.

17. The identity of $\mathbb{Q}^*$ is 1. $\forall\, a/b \in \mathbb{Q}^* : b/a \in \mathbb{Q} : \quad a/b \cdot b/a = 1$, so all of $\mathbb{Q}^*$ have inverses.

18. $\{\pm 1\} \times \mathbb{Q}^* \times \{\pm 1\}$ have inverses.

19. $\{1,3\}$ have inverses.

20. a. $|\mathrm{M}_2\, \mathbb{Z}_2| = |\mathbb{Z}_2|^{2^2} = 2^4 = 16$.

b. Under matrix multiplication, the identity is obviously the identity matrix, and all matrices with nonzero determinant have an inverse:

$$\left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0{,}1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0{,}1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0{,}1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0{,}1 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

21. $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} : n \mapsto (n,0)$ is obviously a homomorphism, and has $\phi 1 = (1,0) \neq 0', 1'$.

22. For det to be a ring homomorphism, it must preserve addition as well, but

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad 1 + 1 = 2 \neq 4,$$

so it is not even a group homomorphism.

23. By Theorem 4.5.12, since $\mathbb{Z}$ is free on $\{\pm 1\}$, $\phi_i : \mathbb{Z} \to \mathbb{Z} : \begin{cases} 0 \mapsto 0 \\ 1 \mapsto i \end{cases} : a \mapsto ia$ are all the group homomorphisms.

$\forall a, b \in \mathbb{Z} : \phi(ab) = \phi a \cdot \phi b \quad \Rightarrow i(ab) = ia \cdot ib = i^2 ab \quad \Rightarrow i = 0 \vee i = 1$, so the only ring homomorphisms are trivial or the identity.

24. From Exercise 23, the ring homomorphisms are $\phi_{ij} : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} : (a,b) \mapsto (ia, jb), \quad i, j = 0, 1$.

25. The projection maps π_i (Example 25) or the trivial homomorphism.

26. From Exercise 25, there are $3 + 1 = 4$.

27. The problem is that $ab = 0 \not\Rightarrow a = 0 \vee b = 0$. For example, $\begin{bmatrix} 1 & & \\ & & \\ & & \end{bmatrix} \cdot \begin{bmatrix} & & \\ & & \\ & & 1 \end{bmatrix} = \begin{bmatrix} 0 & & \\ & 0 & \\ & & 0 \end{bmatrix}$.

28. Is there some more effective way to do this?

$$x^2 + x - 6 = 0 \Rightarrow (x-2)(x+3) \in 14\mathbb{Z} \quad \Rightarrow \begin{cases} (x-2)(x+3) = 0 \\ (x-2)(x+3) = n \cdot 14 \end{cases} \quad \Rightarrow \begin{cases} x = 2 \vee x = -3 = 11 \\ \end{cases}$$

$$\begin{cases} \ldots \\ x - 2 \in 7\mathbb{Z} \wedge x + 3 \in 2\mathbb{Z} \\ x - 2 \in 2\mathbb{Z} \wedge x + 3 \in 7\mathbb{Z} \end{cases} \Rightarrow \begin{cases} \\ x \in \{2,9\} \cap \{1,3,5,\ldots,11\} \\ x \in \{0,2,4,\ldots,12\} \cap \{4,11\} \end{cases} \Rightarrow \begin{cases} x = 2{,}11 \\ x = 9 \\ x = 4 \end{cases} \Rightarrow x \in \{2,4,9,11\}$$

29. That is the definition for a division ring. A field also needs commutative multiplication.

30. The concept of “magnitude” has not been defined in the context of a ring. A unit in a ring is an element with a multiplicative inverse.

31. $2{,}3 \in \mathbb{Z}_6 : 2 \cdot 3 = 0$.

32. $\mathbb{Z}_6$ has multiplicative identity 1, $\langle 3 \rangle \subset \mathbb{Z}_6$ has identity 3.

33. a. true (a field is a commutative division ring)

b. false ($2\mathbb{Z}$, by Exercise 7)

c. false (E)
d. false ($\mathbb{R}$)
e. true ($2\mathbb{Z} \subset \mathbb{Z}$)
f. false (they relate its two operations)
g. true (by Definition 16)
h. true (the operation is associateive by definition of ring, the identity exists and is nonzero by definition of field, and every nonzero element has an inverse by definition of division ring)
i. true (by Definition 1)
j. true (because a ring is an additive group)

34. • (associative) $\forall f, g, h \in F : \forall x \in \mathbb{R}:$
$\left(f\left(gh\right)\right)x = fx \cdot \left(gh\right)x = fx \cdot gx \cdot hx = \left(fg\right)x \cdot hx = \left(\left(fg\right)h\right)x \quad \Rightarrow f\left(gh\right) = \left(fg\right)h$
• (distributive) 'Left distributivity' follows from $\forall f, g, h \in F : \forall x \in \mathbb{R}:$
$\left(f \cdot \left(g+h\right)\right)x = fx \cdot \left(g+h\right)x = fx \cdot \left(gx + hx\right) = fx \cdot gx + fx \cdot hx = \left(fg\right)x + \left(fh\right)x = \left(fg + fh\right)x \Rightarrow f \cdot \left(g+h\right) = fg + fh$
and right distributivity be a similar evaluation.

35. $\forall f, g \in F : \forall x \in \mathbb{R}: \quad \phi_x\left(fg\right) = \left(fg\right)x = fx \cdot gx = \phi_x f \cdot \phi_x g$

36. • (reflexivity) Obviously under the identity isomorphism $\forall a,b \in R: \quad i\left(ab\right) = ab = ia \cdot ib$.
• (symmetry) Let $\phi : R \to R'$ be a ring isomorphism. $\forall a', b' \in R' : \exists a,b \in R : \phi a = a', \phi b = b'$:
$\phi\left(ab\right) = \phi a \cdot \phi b = a' \cdot b' \quad \Rightarrow \phi^{\text{inv}}\left(a'b'\right) = \phi^{\text{inv}}\phi\left(ab\right) = ab = \left(\phi^{\text{inv}}\phi\right)a \cdot \left(\phi^{\text{inv}}\phi\right)b = \phi a' \cdot \phi b'$
so $\phi^{\text{inv}} : R' \to R$ is a ring isomorphism also.
• (transitivity) $\forall \phi : R \to R', \psi : R' \to R'' : \forall a,b \in R:$
$\phi\left(ab\right) = \phi a \cdot \phi b \quad \Rightarrow \left(\psi\phi\right)\left(ab\right) = \psi\left(\phi\left(ab\right)\right) = \psi\left(\phi a \cdot \phi b\right) = \psi\left(\phi a\right) \cdot \psi\left(\phi b\right) = \left(\psi\phi\right)a \cdot \left(\psi\phi\right)b$.

37. • (closure) $\forall a,b \in U : \exists a', b' \in R : aa' = 1, bb' = 1 \quad \Rightarrow \left(ab\right) \cdot \left(b'a'\right) = abb'a' = aa' = 1 \quad \Rightarrow ab \in U$.
• (associativity) by definition of a ring
• (identity) $1 \in R: \quad 1 \cdot 1 = 1 \quad \Rightarrow 1 \in U$.
• (inverse) $\forall a \in U : \exists a' \in U : aa' = 1 \quad \Rightarrow a' \in U$.
so U is a group.

38. $\left(a+b\right)\left(a-b\right) = \left(a+b\right)\left(a+\left(-b\right)\right) = \left(a+b\right)a + \left(a+b\right)\left(-b\right) = a \cdot a + b \cdot a + a \cdot \left(-b\right) + b \cdot \left(-b\right) = a^2 - b^2 + b \cdot a - a \cdot b$
$= a^2 - b^2 \quad \Leftrightarrow b \cdot a - a \cdot b = 0 \quad \Leftrightarrow a \cdot b = b \cdot a$

39. Clearly this multiplication is associative and distributive, and hence forms a ring.

40. $2\mathbb{Z}$ has an element such that $a \cdot a = a + a$ (for $a = 2$), while $3\mathbb{Z}$ does not. $\mathbb{C}$ has an element of multiplicative order 4 (i), while $\mathbb{R}$ does not.

41. Since $\mathbb{Z}_p$ is distributive and commutative, the binomial expansion holds: $\left(a+b\right)^n = +_i \binom{n}{i} a^i b^{n-i}$. So
$\left(a+b\right)^p = +_{0 \le i \le p} \binom{p}{i} a^i b^{p-i} = a^p + b^p +_{0<i<p} a^i b^{p-i}$. Now since p is prime, $\binom{p}{i} = \frac{p!}{\left(p-i\right)!i!}$ is always a multiple of p for $0 < i < p$, so that any such term is always zero.

42. A field is some closed collection of units of a ring, and by Exercise 37 forms a group under multiplication, so the identity of any of its subgroups is its identity.

43. By Exercise 37, $\langle U, \cdot \rangle$ is a group, which has unique inverses.

44. a. $\forall a,b \in R : a^2 = 1, b^2 = 1 : \quad \left(ab\right)^2 = \left(ab\right)\left(ab\right) = abab = aabb = a^2b^2 = 1$.
b. $\left(\{0,1,3,4\}, \{0,1,4,9\}\right)$.

45.

46. $\forall a,b \in R : \exists n,m \in \mathbb{N}^+ : a^n, b^m = 0 \quad \Rightarrow \left(ab\right)^{nm} \overset{\text{commutative}}{=} a^{nm}b^{nm} = 0^m 0^n = 0$ is easy. How about $a+b$?

47. $\Rightarrow \exists x \neq 0 : x^2 = 0 \Rightarrow x$ is nilpotent

$$\Leftarrow \exists x \neq 0 : x \text{ is nilpotent} \quad \Rightarrow \exists \text{minimal } n \neq 0, x^n = 0 \quad \Rightarrow \begin{cases} n \text{ even} : \left(x^{\frac{1}{2}n} \right)^2 = 0, x^{\frac{1}{2}n} \neq 0 \\ n \text{ odd} : x^{n+1} = x^n x = 0 \Rightarrow \left(x^{\frac{1}{2}(n+1)} \right)^2 = 0, x^{\frac{1}{2}(n+1)} \neq 0 \end{cases}$$

48. $\Rightarrow$(additive identity) $0 \in S$

- (additive inverse) $\forall a,b \in S : a - b \in S \quad \Rightarrow 0 - b = 0 + (-b) = -b \in S$
- (additive closure) $\forall a,b \in S \quad \Rightarrow -b \in S \quad \Rightarrow a - (-b) = a + b \in S$

So S is a subgroup.

- (multiplicative closure) $\forall a,b \in S : ab = S$
- (multiplicative associativity, distributivity) follow because R is a ring.

So S is a subring.

49. a. Let $R_{1,2} \subseteq R$ be subrings. From Exercise 48,

$$0 \in R_1, 0 \in R_2 \quad \Rightarrow 0 \in R_1 \cap R_2$$

$$\forall a,b \in R_1 \cap R_2 \quad \Rightarrow a,b \in R_1 \wedge a,b \in R_2 \quad \Rightarrow a - b \in R_1 \wedge a - b \in R_2 \quad \Rightarrow a - b \in R_1 \cap R_2$$

$$\Rightarrow ab \in R_1 \wedge ab \in R_2 \quad \Rightarrow ab \in R_1 \cap R_2$$

so $R_1 \cap R_2$ is a subring.

b. If R is a field, then it is multiplicatively commutative and every element has a multiplicative inverse. Obviously, multiplication remains commutative in $R_1 \cap R_2$ and becuase it is closed, every element has an inverse in $R_1 \cap R_2$. So it is a subfield.

50. Using Exercise 48. $\forall x,y \in I_a$,

$$a0 = 0 \quad \Rightarrow 0 \in I_a$$

$$ax, ay = 0 \quad \Rightarrow a(x - y) = ax - ay = 0 \quad \Rightarrow x - y \in I_a$$

$$a(xy) = (ax) \cdot y = 0y = 0 \quad \Rightarrow xy \in I_a$$

so $I_a \subseteq R$ is a subring.

51.

52. Consider the isomorphism from Example 15 $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s : x \mapsto x(1,1)$. Obviously $\pi_0\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r : x \mapsto x \bmod r$ and $\pi_1\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_s : x \mapsto x \bmod s$. So the problem amounts to finding x such that $\pi_0\phi x = m \bmod r, \quad \pi_1\phi x = n \bmod s$, i.e. $\phi x = (m \bmod r, n \bmod s) \in \mathbb{Z}_r \times \mathbb{Z}_s$. Since ϕ is an isomorphism and thus surjective, such an x exists.

53. a. For a set $S = \{_i \; s_i\}$ of relatively prime positive integers. By the Fundamental Theorem of commutative groups, $\mathbb{Z}_{\cdot_i s_i} \cong \times_i \mathbb{Z}_{s_i}$ are group isomorphic. Since they are generated by 1 and $(_i \; 1)$ respectively, with Theorem 4.5.12 $\phi : \mathbb{Z}_{\cdot_i s_i} \to \times_i \mathbb{Z}_{s_i} : x \mapsto x(_i \; 1)$ is a group isomorphism. Multiplicative isomorphism follows from $\forall x,y \in \mathbb{Z}_{\cdot_i s_i} : \phi(xy) = (xy) \cdot (_i \; 1) = (_i \; xy) = (_i \; x) \cdot (_i \; y) = x(_i \; 1) \cdot y(_i \; 1) = \phi x \cdot \phi y$. So ϕ is a ring isomorphism.

b. Let $r_i, s_i \in \mathbb{N}^*$ with r_i relatively prime, show that $\exists x \in \mathbb{Z}^+ : \forall i : x =_{s_i} r_i$. Consider the isomorphism of (a.), $\phi : \mathbb{Z}_{\cdot_i s_i} \to \times_i \mathbb{Z}_{s_i}$. Obviously $\pi_i\phi : \mathbb{Z}_{\cdot_i s_i} \to \mathbb{Z}_{s_i} : x \mapsto x \bmod s_i$, so the problem amounts to finding x such that $\pi_i\phi x = r_i \bmod s_i$, i.e. $\phi x = (_i \; r_i \bmod s_i) \in \times_i \mathbb{Z}_{s_i}$. Since ϕ is an isomorphism and thus surjective, such an x exists.

54.
- (additively commutative) $\forall a,b \in S$:

$$(1+1)(a+b) = \begin{cases} (1+1)a + (1+1)b = a + a + b + b \\ 1(a+b) + 1(a+b) = a + b + a + b \end{cases} \Rightarrow a + a + b + b = a + b + a + b \quad \Rightarrow a + b = b + a$$

so S is a commutative group.

- (multiplicative associativity) Even though we haven't shown S is a ring, the proof of Theorem 8 shows that multiplication is associative when either of the operands is 0, so multiplication is associative over all of S^* (that is, *including* the additive identity).

Distributivity holds by axiom, so S is a ring.

- (multiplicative identity and inverse) Since S^* is a group, it has an identity not the same as the additive identity, and

each element has an inverse.
So S is a division ring.

55. Since every element is idempotent, $\forall a \in R$:

$$(a+1)(a+1) = \begin{cases} a+1 \\ a^2 + a + a + 1 = a + a + a + 1 \end{cases} \Rightarrow a+1 = a+a+a+1 \quad \Rightarrow a+a=0 \quad \Rightarrow a=-a$$

so then $\forall a,b \in R$

$$(a+b)(a+b) = \begin{cases} a+b \\ a^2 + ab + ba + b^2 = a + ab + ba + b \end{cases} \Rightarrow a+b = a+ab+ba+b \quad \Rightarrow ab+ba=0 \quad \Rightarrow ab = -(ba) = ba$$

so R is commutative.

56. $S = \{a,b\}, \quad \mathrm{P}S = \{\varnothing,\{a\},\{b\},\{a,b\}\}$.

a.

$+$	$\varnothing$	a	b	ab
$\varnothing$	$\varnothing$	a	b	ab
a	a	$\varnothing$	ab	b
b	b	ab	$\varnothing$	a
ab	ab	b	a	$\varnothing$

$\cdot$	$\varnothing$	a	b	ab
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
a	$\varnothing$	a	$\varnothing$	a
b	$\varnothing$	$\varnothing$	b	b
ab	$\varnothing$	a	b	ab

b. We show that $\mathrm{P}S \cong \mathbb{B}^{|S|}$ by $\phi : \mathbb{B}^{|S|} \to \mathrm{P}S : ({}_i\, b_i) \mapsto \{s_i \in S \mid b_i = 1\}$.

- (additively homomorphic) $\forall x,y \in \mathbb{B}^{|S|}$:

$$\begin{aligned}\phi(x+y) &= \{s_i \in S \mid (x+y)_i = 1 \quad \Rightarrow x_i + y_i = 1 \quad \Rightarrow x_i = 1 \vee y_i = 1 \wedge x_i \neq y_i\} \\ &= \{s_i \in S \mid x_i = 1\} \cup \{s_i \in S \mid y_i = 1\} \setminus \{s_i \in S \mid x_i = 1\} \cap \{s_i \in S \mid y_i = 1\} \\ &= \{s_i \in S \mid x_i = 1\} + \{s_i \in S \mid y_i = 1\} = \phi x + \phi y\end{aligned}$$

- (multiplicatively homomorphic) $\forall x,y \in \mathbb{B}^{|S|}$:

$$\begin{aligned}\phi(xy) &= \{s_i \in S \mid (xy)_i = 1 \quad \Rightarrow x_i y_i = 1 \quad \Rightarrow x_i = 1 \wedge y_i = 1\} \\ &= \{s_i \in S \mid x_i = 1\} \cap \{s_i \in S \mid y_i = 1\} \\ &= \{s_i \in S \mid x_i = 1\} \cdot \{s_i \in S \mid y_i = 1\} = \phi x \cdot \phi y\end{aligned}$$

So ϕ is a ring homomorphism. Clearly $\phi x = \varnothing \Rightarrow x = 0 \Rightarrow \ker\phi = E$ and $\forall S \in \mathrm{P}S : \exists x \in \mathbb{B}^{|S|} : \phi x = S$, so ϕ is injective and surjective, so ϕ is a ring isomorphism.

Now $\forall b \in \mathbb{B}^n : b^2 = b \cdot b = ({}_i\, b_i \cdot b_i) = ({}_i\, b_i) = b$ so $\mathbb{B}^{|S|}, \mathrm{P}S$ are boolean rings.

§5.2 Integral Domains

1. $x^3 - 2x^2 - 3x = x(x^2 - 2x - 3) = x(x-3)(x+1) \in \mathbb{Z}_{12}$. This holds if any of the factors is 0, or the product contains the factors of $12 = 2 \cdot 2 \cdot 3$. It seems easier to just try $x \in \{0,3,5,8,9,11\}$.

2. $3x =_7 2 \quad \Leftarrow x =_7 2/3 =_7 2 \cdot 3^{-1} =_7 2 \cdot 5 =_7 10 =_7 3$. Since 3 does not divide 7, there are no other solutions.
$3x =_{23} 2 \quad \Leftarrow x =_{23} 2/3 =_{23} 2 \cdot 3^{-1} =_{23} 2 \cdot 8 =_{23} 16$. Since 3 does not divide 23, there are no other solutions.

3. $x^2 + 2x + 2 =_6 0 \quad \Leftarrow x = \dfrac{-2 \pm \sqrt{4 - 4 \cdot 2 \cdot 1}}{2} = \dfrac{-2 \pm 2\sqrt{i}}{2}$ has no integer solutions.

4. $x^2 + 2x + 4 = (x+2)^2 =_6 0 \quad \Rightarrow x =_6 -2 =_6 4$. There are no other solutions.

5. $\operatorname{char} 2\mathbb{Z} = 0$; 6. $\operatorname{char} \mathbb{Z} \times \mathbb{Z} = 0$; 7. $\operatorname{char} \mathbb{Z}_3 \times 3\mathbb{Z} = 0$; 8. $\operatorname{char} \mathbb{Z}_3 \times \mathbb{Z}_3 = 3$; 9. $\operatorname{char} \mathbb{Z}_3 \times \mathbb{Z}_4 = 12$;
10. $\operatorname{char} \mathbb{Z}_6 \times \mathbb{Z}_{15} = 30$.

11. $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 = a^4 + 2a^2b^2 + b^4$.

12. $(a+b)^9 = \left((a+b)^3\right)^3 = (a^3 + 3a^2b + 3ab^2 + b^3)^3 = (a^3 + b^3)^3 = (a^3)^3 + 3(a^3)^2(b^3) + 3(a^3)(b^3)^2 + (b^3)^2 = a^9 + b^9$.

13. $(a+b)^6 = \left((a+b)^3\right)^2 = \left(a^3+3a^2b+3ab^2+b^3\right)^2 = \left(a^3+b^3\right)^2 = \left(a^3\right)^2 + 2\left(a^3b^3\right) + \left(b^3\right)^2 = a^6 + 2a^3b^3 + b^6$.

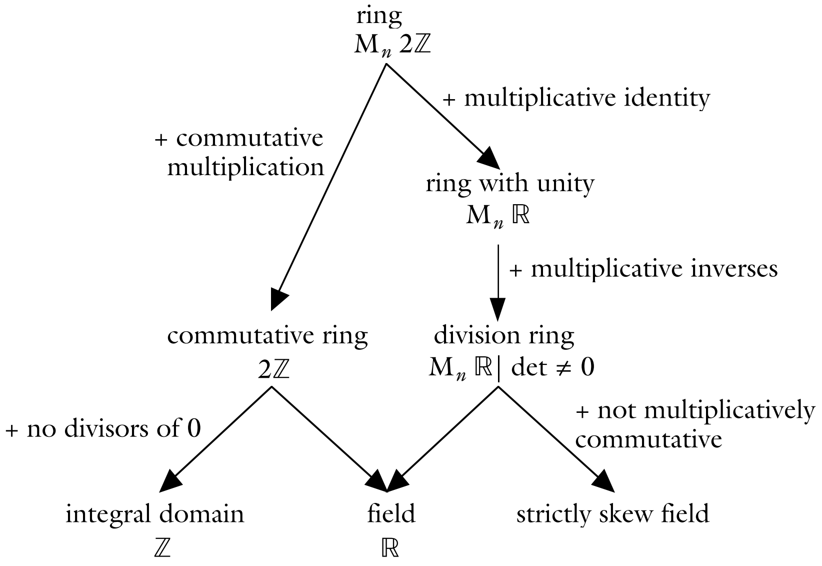
14. $\det\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = 0$ so the row vectors are linearly dependent: $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

15. "If $a,b \in R$ are elements of a ring R…"

16. "If n is the least positive integer…"

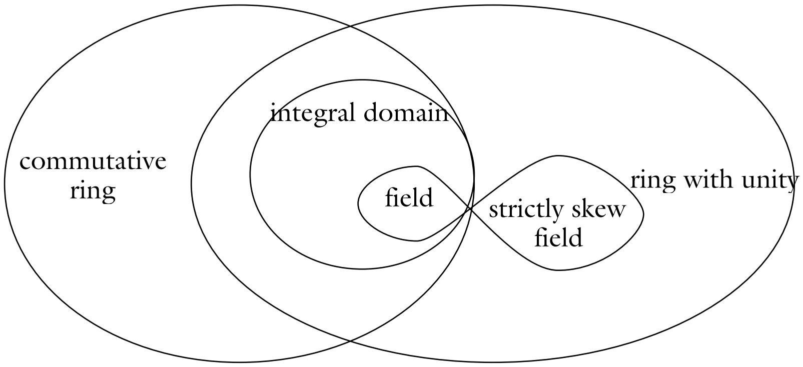
17. a. false ($n\mathbb{Z}$ does not have a multiplicative identity for $n > 1$)
b. true (Theorem 9)
c. false (they all have characteristic 0)
d. false ($\mathbb{Z}$ has multiplicative inverse but $2\mathbb{Z}$ doesn't)
e. true (Definition 6 and Theorem 5)
f. true (if it was finite $n \cdot a = 0$ for some $n \in \mathbb{R}$)
g. false (Example 7)
h. true ($\forall a: \exists b: ab = 0: \exists c: ac = 1 \Rightarrow ab + ac = 1 \Rightarrow a(b+c) = 1$ and because the inverse is unique, $b + c = c \Rightarrow b = 0$ so a would not be a divisor of 0)
i. false ($n\mathbb{Z}$ does not have a multiplicative identity for $n > 1$)
j. false ($\mathbb{Z}$ is not a division ring or a field)

18.



19. The matrix is not invertible, has a zero determinant, linearly dependent row or column vectors. (Book says something about eigenvalues.)

20.



21. $\forall a \in R^*: a^2 = a \Rightarrow aa = a \Rightarrow aaa^{-1} = aa^{-1} \Rightarrow a1 = 1 \Rightarrow a = 1$. Also, for $0 \in R: 0^2 = 0$. So the additive and multiplicative identities are the only idempotent elements of a division ring.

22. By Exercise 1.49a, an intersection of rings is a ring, and therefore an intersection of commutative rings is again a commutative ring. Since the multiplicative identity is unique, it is contained in each of the domains and hence in

their intersection. Finally, none of the domains have divisors of zero so neither does the intersection. Therefore, the intersection is itself an integral domain.

23. It remains to be shown that each element has a multiplicative inverse. Let $R^* = \{_i\, 1, a_i\}$, and consider $aR^* = \{_i\, a1, aa_i\}$. Each of these elements is distinct, because $aa_i = aa_j \overset{\text{cancellation}}{\Rightarrow} a_i = a_j \Rightarrow i = j$ and $a1 = aa_i \overset{\text{cancellation}}{\Rightarrow} a_i = 1$. Now R has no divisors of zero, so $\nexists a_i : aa_i = 0$. Thus $aR = R$, and either $a1 = 1 \Rightarrow a = 1 \Rightarrow a^{-1} = 1$ or $aa_i = 1 \Rightarrow a^{-1} = a_i$. Suppose $\exists a_j : a_j a = 1 \Rightarrow a_j aa_i = a_i \Rightarrow a_j = a_i$, so the 'left multiplicative inverse' is also the 'right multiplicative inverse'.

24. a. Suppose $\exists a \in R^* : \exists b \in R : ab = 0 \Rightarrow aba = 0a = 0 \neq a$, so R cannot have divisors of 0.

b. $\forall a \in R^* : \exists b \in R : aba = a \Rightarrow abab = ab \Rightarrow abab - ab = 0 \overset{\text{cancellation}}{\Rightarrow} a(bab - b) = 0 \overset{\substack{\text{no divisors}\\ \text{of } 0}}{\Rightarrow} bab = b$. If $b = 0 \Rightarrow a = aba = a0a = 0$, so $b \in R^*$.

c.

d. $\forall a \in R^* : \exists b \in R^* : aba = a \Rightarrow aba - a = a(ba - 1) = 0 \Rightarrow ba = 1 \Rightarrow a^{-1} = b$.

25. Using Theorem 15, the smallest n such that $n \cdot 1 = 0$ must be the same in any subdomain.

26. $\{_{n \in \mathbb{Z}}\, n \cdot 1\} \subseteq D$ is a commutative ring with unity and no divisors of 0, so is itself an integral domain. Since any subdomain of D contains unity and is closed under addition, it must certainly contain $\{_{n \in \mathbb{Z}}\, n \cdot 1\}$.

27. We know that $\operatorname{char}\mathbb{Z} = 0$. Suppose that $\exists D : \exists n, m \in \mathbb{N}^+ : \operatorname{char} D = n \cdot m$. Then

$$(n \cdot 1)(m \cdot 1) = (+_{i<n}\, 1)(+_{i<m}\, 1) \overset{\text{distributive}}{=} +_{i<n}\, (1 \cdot +_{i<m}\, 1) \overset{\text{distributive}}{=} +_{i<nm}\, 1 \cdot 1 = +_{i<nm}\, 1 = 0$$

and (Theorem 15) $n \cdot 1, m \cdot 1 \neq 0$, which would show that D has divisors of 0. So the characteristic has to be prime or 0.

28. a. It is fairly obvious that multiplication is closed on S, and we know that S is a commutative group because R and $\mathbb{Z}_n$ are. Multiplicative associativity follows directly from the definition by observing that swapping indices yields the same expression. Multiplicative distributivity obviously holds for the second component. For the first, $\forall (r_1, n_1), (r_2, n_2), (r_3, n_3) \in R \times \mathbb{Z}_n$:

$$\begin{aligned}
(r_1, n_1) \cdot ((r_2, n_2) + (r_3, n_3)) &= (r_1, n_1) \cdot (r_2 + r_3, n_2 + n_3) \\
&= (r_1(r_2 + r_3) + n_1 \cdot (r_2 + r_3) + (n_2 + n_3) \cdot r_1, n_1(n_2 + n_3)) \\
&= (r_1 r_2 + r_1 r_3 + n_1 r_2 + n_1 r_3 + n_2 r_1 + n_3 r_1, n_1 n_2 + n_1 n_3) \\
&= (r_1 r_2 + n_1 r_2 + n_2 r_1, n_1 n_2) + (r_1 r_3 + n_1 r_3 + n_3 r_1, n_1 n_3) \\
&= (r_1, n_1)(r_2, n_2) + (r_1, n_1)(r_3, n_3)
\end{aligned}$$

Surely right distributivity follows similarly. So S is a ring.

b. $\exists (r_1, n_1) : \forall (r_2, n_2) : (r_1, n_1) \cdot (r_2, n_2) = (r_2, n_2) \Rightarrow (r_1 r_2 + n_1 r_2 + n_2 r_1, n_1 n_2) = (r_2, n_2)$

$$\Rightarrow \begin{cases} n_1 = 1 \\ r_1 r_2 + r_2 + n_2 r_1 = r_2 \Rightarrow r_1 r_2 + n_2 r_1 = r_1(r_2 + n_2 1) = 0 \Rightarrow r_1 = 0 \end{cases}$$

so $1_S = (0, 1)$.

c. The characteristic of S is the minimal n such that $n \cdot 1_S = 0 \Leftrightarrow n \cdot (0, 1) = 0 \Leftrightarrow n \cdot 1_{\mathbb{Z}_n} = 0$, which is the characteristic of $\mathbb{Z}_n$ by axiom.

d. Show that ϕ is a ring isomorphism so that $\phi R \subseteq S$ is a ring. $\forall r_1, r_2$:

$\phi r_1 = \phi r_2 \Rightarrow (r_1, 0) = (r_2, 0) \Rightarrow r_1 = r_2$ (injective)

$\phi(r_1 + r_2) = (r_1 + r_2, 0) = (r_1, 0) + (r_2, 0) = \phi r_1 + \phi r_2$ (group homomorphism)

$\phi(r_1 \cdot r_2) = (r_1 \cdot r_2, 0) = (r_1 \cdot r_2 + 0 \cdot r_2 + 0 \cdot r_1, 0) = (r_1, 0) \cdot (r_2, 0) = \phi r_1 \cdot \phi r_2$ (ring homomorphism)

29. There are $|\mathbb{Z}_3|^4 = 3^4 = 81$ code words and $|\mathbb{Z}_3|^2 = 9$ message words. (Note that the terminology used in this exercise appears to be inconsistent with that in §2.5).

30. There are $|F|^4 = 16^4 = 2^{16} = 65536$ code words and $|F|^2 = 16^2 = 2^8 = 256$ message words.

§5.3 Fermat's and Euler's Theorems

1. $\langle 3\rangle = \left\{3^0 =_7 1, 3^1 =_7 3, 3^2 =_7 2, 3^3 =_7 6, 3^4 =_7 4, 3^5 =_7 5, 3^6 =_7 1\right\} = \mathbb{Z}_7{}^*$

2. $\langle 4\rangle = \left\{4^0 =_{11} 1, 4^1 =_{11} 4, 4^2 =_{11} 5, 4^3 =_{11} 9, 4^4 =_{11} 3, 4^5 =_{11} 1\right\} \neq \mathbb{Z}_{11}{}^*$

$\langle 3\rangle = \left\{3^0 =_{11} 1, 3^1 =_{11} 3, 3^2 =_{11} 9, 3^3 =_{11} 5, 3^4 =_{11} 4, 3^5 =_{11} 1\right\} \neq \mathbb{Z}_{11}{}^*$

$\langle 2\rangle = \left\{2^0 =_{11} 1, 2^1 =_{11} 2, 2^2 =_{11} 4, 2^3 =_{11} 8, 2^4 =_{11} 5, 2^5 =_{11} 10, 2^6 = 9, 2^7 = 7, 2^8 =_{11} 3, 2^9 =_{11} 6, 2^{10} =_{11} 1\right\} = \mathbb{Z}_{11}{}^*$

3. $\langle 2\rangle = \left\{2^0 =_{17} 1, 2^1 =_{17} 2, 2^2 =_{17} 4, 2^3 =_{17} 8, 2^4 =_{17} 16, 2^5 =_{17} 15, 2^6 =_{17} 13, 2^7 =_{17} 9, 2^8 =_{17} 1\right\} \neq \mathbb{Z}_{17}{}^*$

$\langle 3\rangle = \{3^0 =_{17} 1, 3^1 =_{17} 3, 3^2 =_{17} 9, 3^3 =_{17} 10, 3^4 =_{17} 13, 3^5 =_{17} 5, 3^6 =_{17} 15, 3^7 =_{17} 11,$

$3^8 =_{17} 16, 3^9 =_{17} 14, 3^{10} =_{17} 8, 3^{11} =_{17} 7, 3^{12} =_{17} 4, 3^{13} =_{17} 12, 3^{14} =_{17} 2, 3^{15} =_{17} 6, 3^{16} =_{17} 1\} = \mathbb{Z}_{17}{}^*$

4. $3^{47} =_{23} \left(3^{22}\right)^2 3^3 =_{23} 1^2 \cdot 3^3 =_{23} 27 =_{23} 4$.

5. $37^{49} =_7 \left(37^6\right)^8 37^1 =_7 1^8 \cdot 37^1 =_7 37 =_7 2$.

6. $2^{2^{17}} =_{19} 2^{n\cdot 18+14} =_{19} \left(2^{18}\right)^n 2^{14} =_{19} 1^n 2^{14} =_{19} 2^{14} =_{19} \left(2^4\right)^3 2^2 =_{19} (-3)^3 4 =_{19} -27\cdot 4 =_{19} 11\cdot 4 =_{19} 44 =_{19} 6$

$\Leftarrow \quad 2^{17} = a\cdot 18 + b \Rightarrow 2^{16} = a\cdot 9 + \frac{1}{2}b$

$2^{16} =_9 \left(2^6\right)^2 \cdot 2^4 =_9 1^2 2^4 =_9 7 \Rightarrow 2^{17} =_{18} 14$

$2^{2^{17}} + 1 =_{19} 6 + 1 =_{19} 7$

7.

	0x	1x	2x	3x
x0		4	8	8
x1	1	10	12	
x2	1	4	10	
x3	2	12	22	
x4	2·1 = 2	6	8	
x5	4	8	5·4 = 20	
x6	2	8	12	
x7	6	16	18	
x8	4	6	12	
x9	3·2 = 6	18	28	

8. $\varphi p^2 = p(p-1)$.

9. $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

10. $7^{1000} =_{24} \left(7^8\right)^{125} =_{24} \left(7^{\varphi 24}\right)^{125} =_{24} 1^{125} = 1$.

11. $2x =_4 6 \Rightarrow x =_2 3 \Rightarrow x \in \left\{_{k\in\{0,1\}}(3 + k\cdot 2) + 4\mathbb{Z}\right\}$.

12. $22x =_{15} 5 \Leftrightarrow 7x =_{15} 5 \Rightarrow x =_{15} 7^{-1}5 =_{15} 55 =_{15} 10$

$7\cdot(1,2,4,7,8,11,13,14) =_{15} (7,14,13,4,11,2,1,8) \Rightarrow 7^{-1} =_{15} 11$

$10 + 15\mathbb{Z}$

13. $36x =_{24} 15$; $\gcd(36,12) =_{15} 12, 15 =_{12} 3 \neq 0$.

14. $45x_{24}15 \Rightarrow 15x =_8 5 \Rightarrow 7x =_8 5 \Rightarrow x =_8 7^{-1}5 =_8 7 \cdot 5 = 35 =_8 3$
$7 \cdot (1,3,5,7) = (7,21,35,49) =_8 (7,5,3,1) \Rightarrow 7^{-1} =_8 7$
$x \in \{3 + 3\mathbb{Z}\} + 8\mathbb{Z}$

15. $39x =_9 125$; $\gcd(39,9) = 3, 125 =_3 1 \neq 0$.

16. $41x =_9 125 \Rightarrow 5x =_9 8$
$5 \cdot (1,2,4,5,7,8) = (5,10,20,25,35,40) =_9 (5,1,2,7,8,4) \Rightarrow 5^{-1} =_9 2$
$x =_9 5^{-1} \cdot 8 =_9 2 \cdot 8 = 16 =_9 7$
$x \in \{7 + 9\mathbb{Z}\}$

17. $155x =_{65} 75 \Rightarrow 31x =_{13} 15 \Rightarrow 5x =_{13} 2$
$5 \cdot 8 = 40 =_{13} 1 \Rightarrow 5^{-1} =_{13} 8$
$x =_{13} 5^{-1}2 =_{13} 8 \cdot 2 = 16 =_{13} 3$
$x \in \{3 + 13\mathbb{Z}\}$

18. $39x =_{130} 52 \Rightarrow 3x =_{10} 4$
$3 \cdot 7 = 21 =_{10} 1 \Rightarrow 3^{-1} =_{10} 7$
$x =_{10} 3^{-1}4 =_{10} 7 \cdot 4 = 28 =_{10} 8$
$x \in \{8 + 10\mathbb{Z}\}$

19. By Exercise 26, $(p-1)! =_p -1 \Rightarrow (p-1)(p-2)! = -1 = p - 1 \Rightarrow (p-2)! =_p 1$.

20. $(37-2)! =_{37} 35! =_{37} 35 \cdot 34! =_{37} 1 \Rightarrow 34! =_{37} 35^{-1} = (5 \cdot 7)^{-1} = 5^{-1}7^{-1} =_{37} 15 \cdot 16 = 240 =_{37} 18$
$5 \cdot 15 = 75 =_{37} 1 \Rightarrow 5^{-1} =_{37} 15$
$7 \cdot 16 = 112 =_{37} 1 \Rightarrow 7^{-1} =_{37} 16$

21. $51! = 51 \cdot 50 \cdot 49! \overset{\text{(Ex 19)}}{=_{53}} 1 \Rightarrow 49! =_{53} (51 \cdot 50)^{-1} =_{53} 6^{-1} = 9$
$51 \cdot 50 = 2550 =_{53} 430 =_{53} 6$
$9 \cdot 6 = 54 =_{53} 1 \Rightarrow 6^{-1} = 9$

22. $(29-2)! = 27! = 27 \cdot 26 \cdot 25 \cdot 24! \overset{\text{(Ex 19)}}{=_{29}} 1 \Rightarrow 24! =_{29} (27 \cdot 26 \cdot 25)^{-1} =_{29} 17^{-1} =_{29} 8$
$27 \cdot 26 \cdot 25 = 27 \cdot 650 =_{27} 27 \cdot 2 = 54 =_{27} 17$
$8 \cdot 17 = 136 =_{53} 1 \Rightarrow 17^{-1} = 8$

23. a. false ($a \neq_p 0 \Leftrightarrow p$ does not divide a)
b. true
c. true (by definition)
d. false ($\varphi 1 = 1 \not\leq 1 - 1 = 0$)
e. true
f. true (a product of two relatively prime numbers is still relatively prime)
g. false (the product will not be relatively prime)
h. true
i. false (if $a = p \Rightarrow ax =_p px =_p 0 \neq b$)
j. true (what is an "incongruent solution?")

24. The units of $\mathbb{Z}_{12}$ are 1, 5, 7, and 11.

1	5	7	11
5	1	11	7
7	11	1	5
11	7	5	1

Its multiplicative group is isomorphic to the Klein 4-group.

25. Let $x \in \mathbb{Z}_p : x^2 = 1 \Rightarrow x^2 - 1 = 0 \Rightarrow x^2 + x - x - 1 \overset{\text{(ring)}}{=} x(x+1) - x(x+1) \overset{\text{(ring)}}{=} (x-1)(x+1) = 0$. By Corollary 2.4, $\mathbb{Z}_p$ has no divisors of 0, so $x =_p 1 \vee x =_p -1 = p-1$.

26. Since p is odd, $p-1$ is even, so $\left|\{2,\ldots,p-2\}\right|$ is also even. Since by Exercise 25, 1 and $p-1$ are the only elements who are their own inverses, the even number elements in $\{2,\ldots,p-2\}$ each have their inverses in that same subset, so ${\cdot}_{i=2}^{p} i = p! =_p 1$ (cf. Exercise 19), so $(p-1)! = (p-1)(p-2)! = (p-1) =_p -1$.

$383838 = 37 \cdot 19 \cdot 13 \cdot 7 \cdot 3 \cdot 2$

27.
$$\left.\begin{aligned}
n^{37} - n &= \left(n^{36}\right)^{1} n - n =_p n - n = 0 \\
n^{37} - n &= \left(n^{18}\right)^{2} n - n =_p n - n = 0 \\
n^{37} - n &= \left(n^{12}\right)^{3} n - n =_p n - n = 0 \\
n^{37} - n &= \left(n^{6}\right)^{6} n - n =_p n - n = 0 \\
n^{37} - n &= \left(n^{2}\right)^{18} n - n =_p n - n = 0 \\
n^{37} - n &= \left(n^{1}\right)^{36} n - n =_p n - n = 0
\end{aligned}\right\} \Rightarrow n^{37} - n =_{383838} 0.$$

28. $n^{37} - n = \left(n^4\right)^9 n - n =_p \left(n^{5-1}\right)^9 n - n =_p n - n = 0;\ 383838 \cdot 5 = 1919190 \Rightarrow n^{37} - n =_{1919190} 0$.

§5.4 The Field of Quotients of an Integral Domain

1. In the same way that the field of quotients $\mathbb{Z} \times \mathbb{Z}$ was reinterpreted as $\mathbb{Q}$, this field of quotients $D \times D$ can be interpreted as $\mathbb{Q} \times i\mathbb{Q}$.
2. $\mathbb{Q} + \mathbb{Q}\sqrt{2}$?
3. A field is a division ring, in which by definition every nonzero element is a unit. Since the zero of D is the zero of F, that last part of the definition is redundant.
4. a. true

   b. false ($\sqrt{2}$ is not a quotient of $\mathbb{Z}$)

   c. true ($\mathbb{R}/\mathbb{R}^* \subseteq \mathbb{R}$)

   d. false (i is not a quotient of $\mathbb{R}$)

   e. true

   f. true (otherwise + and · could not be defined)

   g. false (see h.)

   h. true (every nonzero element of a division ring is a unit, and a field is a division ring)

   i. true

   j. true (Corollary 9)
5. $2\mathbb{Z} \subset \mathbb{Z}$ is an integral domain. Its field of quotients includes $[(2,4)]$, and $[(2,4)] + [(2,4)] = [(2 \cdot 4 + 4 \cdot 2, 4 \cdot 4)] = [(16,16)] = [(16 \cdot 1, 16 \cdot 1)] = [(1,1)]$, so its field of quotients is at least a subset of $\mathbb{Z} \times \mathbb{Z}$. Similarly, for any element $[(a,b)]$, $a \in \mathbb{Z}, b^* \in \mathbb{Z}$ in the field of quotients of $\mathbb{Z}$, $[(2a,2)], [(2,2b)]$ are in the

field of quotients of $2\mathbb{Z}$ and $[(2a,2)]\cdot[(2,2b)]=[(2a\cdot 2,2\cdot 2b)]=[(4a,4b)]=[(a,b)]$, so the fields of quotients of $\mathbb{Z}$ and $2\mathbb{Z}$ are equal.

6. Prove that addition in F is associative.

$$\begin{aligned}([(a,b)]+[(c,d)])+[(e,f)] &= [(ad+bc,bd)]+[(e,f)]\\ &= [(ad+bc)f+(bd)e,(bd)f]\\ &= [(adf+bcf+bde,bdf)]\\ &= [(a(df)+b(cf+de),b(df))]\\ &= [(a,b)]+[(cf+de,df)]\\ &= [(a,b)]+([(c,d)]+[(e,f)])\end{aligned}$$

7. $[(0,1)]$ is an additive identity in F: $\forall[(a,b)]\in F:[(a,b)]+[(0,1)]=[(a\cdot 1+b\cdot 0,b\cdot 1)]=[(a,b)]$.

8. $[(-a,b)]$ is an additive inverse in F. $\forall[(a,b)]\in F:$

$[(-a,b)]+[(a,b)]=[(-a\cdot b+b\cdot a,b\cdot b)]=[((-a+a)\cdot b,b\cdot b)]=[(0\cdot b,b\cdot b)]=[(0,b\cdot b)]=[(0,1)]$

$\Leftarrow 0\cdot 1=(b\cdot b)\cdot 0\Leftrightarrow 0=0$

9. Multiplication in F is associative. $\forall[(a,b)],[(c,d)],[(e,f)]\in F:$

$([(a,b)]\cdot[(c,d)])\cdot[(e,f)]=[(ac,bd)]\cdot[(e,f)]=[((ac)e,(bd)f)]$

$=[(a(ce),b(df))]=[(a,b)]\cdot[(ce,df)]=[(a,b)]\cdot([(c,d)]\cdot[(e,f)])$

10. Multiplication in F is commutative. $\forall[(a,b),(c,d)]\in F:$

$[(a,b)]\cdot[(c,d)]=[(ac,bd)]=[(ca,db)]=[(c,d)]\cdot[(a,d)]$.

11. Distribution laws hold in F. $\forall[(a,b)],[(c,d)],[(e,f)]\in F:$

$[(a,b)]\cdot([(c,d)]+[(e,f)])=[(a,b)]+[(cf+de,df)]=[(a(cf+de),b(df))]=[(ba(cf+de),bb(df))]$

$=[(bacf+bade,bbdf)]=[(ac\cdot bf+bd\cdot ae,bd\cdot bf)]=[(ac,bd)]+[(ae,bf)]=[(a,b)]\cdot[(c,d)]+[(a,b)]\cdot[(e,f)]$

12. a. $\forall t\in T:[(t,t)]$ is unity.

b. $\forall t,t'\in T:[(t,t')]\cdot[(t',t)]=[(tt',t't)]=1$.

13. By Exercise 12, $\mathrm{Q}(R,\langle a\rangle)$ is a commutative ring with unity.

14. $\mathrm{Q}(\mathbb{Z}_4,\{1,3\})=\left\{\frac{0}{1}=\frac{0}{3},\frac{1}{1}=\frac{3}{3},\frac{2}{1}=\frac{6}{3}=\frac{2}{3},\frac{3}{1}=\frac{9}{3}=\frac{1}{3}\right\}$ has 4 elements.

15. $\mathrm{Q}\left(\mathbb{Z},\left\{_{n\in\mathbb{Z}^+}2^n\right\}\right)$ are all $\left\{_{n\in\mathbb{Z},m\in\mathbb{Z}^+}n/2^m\right\}$.

16. $\mathrm{Q}\left(3\mathbb{Z},\left\{_{n\in\mathbb{Z}^+}6^n\right\}\right)$ are $\{3n/6^n\}=\{3n/6\cdot 6^{n-1}\}=\left\{\frac{1}{2}n/6^{n-1}\right\}=\ldots$ all fractions $n/2^m+o/3^p$.

17.

§5.5 Rings of Polynomials

♥ $R[x]$ is the set of **formal polynomials** with coefficients in R and **indeterminate** *x*. ‘Formal’ means that the indeterminate is to be seen as purely a symbol with no algebraic interpretation. A polynomial is an infinite sum

$f[x] = +_i\ f_i x^i$ with a finite number of nonzero coefficients. $R \subset R[x]$ are the **constant polynomials**. The finiteness enables or simplifies some kinds of operations (see for example P_{high} in the section on ordered rings) but isn't necessary for the polynomial 'concept' itself. In fact, that same section defines **power series rings** and **Laurent series fields** which modify this restriction in different ways.

♥ The evaluation homomorphism assigns a value from some superfield E to the indeterminate: $\phi_a\ +_i\ f_i x^i = +_i\, f_i a^i$.

1. $f[x] = 4x - 5, g[x] = 2x^2 - 4x + 2$ in $\mathbb{Z}_8[x]$:

$$f[x] + g[x] = (4x-5) + (2x^2 - 4x + 2) = 2x^2 + (4-4)x + (-5+2) =_8 2x^2 + 5.$$

$$f[x] \cdot g[x] = (4x-5)(2x^2-4x+2) = 4x(2x^2-4x+2) - 5(2x^2-4x+2)$$
$$= 8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10 = 8x^3 - 26x^2 + 28x - 10 =_8 6x^2 + 4x + 6$$

2. $f[x] = x+1, g[x] = x+1$ in $\mathbb{Z}_2[x]$:

$$f[x] + g[x] = (x+1) + (x+1) = 2x^2 + 2 =_2 0$$

$$f[x] \cdot g[x] = (x+1)(x+1) = x(x+1) + 1(x+1) = x^2 + 2x + 1 =_2 x^2 + 1.$$

3. $f[x] = 2x^2 + 3x + 4, g[x] = 3x^2 + 2x + 3$ in $\mathbb{Z}_6[x]$:

$$f[x] + g[x] = (2x^2+3x+4) + (3x^2+2x+3) = 5x^2 + 5x + 7 =_6 5x^2 + 5x + 1$$

$$f[x] \cdot g[x] = (2x^2+3x+4) \cdot (3x^2+2x+3)$$
$$= 2x^2(3x^2+2x+3) + 3x(3x^2+2x+3) + 4(3x^2+2x+3)$$
$$= 6x^4 + 4x^3 + 6x^2 + 9x^3 + 6x^2 + 9x + 11x^2 + 8x + 12$$
$$= 6x^4 + 13x^3 + 24x^2 + 17x + 12$$
$$=_6 x^3 + 5x$$

4. $f[x] = 2x^3 + 4x^2 + 3x - 2, g[x] = 3x^4 + 2x + 4$ in $\mathbb{Z}_5[x]$:

$$f[x] + g[x] = (2x^3 + 4x^2 + 3x + 2) + (3x^4 + 2x + 4) = 3x^4 + 2x^3 + 4x^2 + 5x + 6 =_5 3x^4 + 2x^3 + 4x^2 + 1$$

$$f[x] \cdot g[x] = (2x^3 + 4x^2 + 3x + 2) \cdot (3x^4 + 2x + 4)$$
$$= 2x^3(3x^4+2x+4) + 4x^2(3x^4+2x+4) + 3x(3x^4+2x+4) + 2(3x^4+2x+4)$$
$$= 6x^7 + 4x^4 + 8x^3 + 12x^6 + 8x^3 + 16x^2 + 9x^5 + 6x^2 + 12x + 6x^4 + 4x + 8$$
$$= 6x^7 + 12x^6 + 9x^5 + 10x^4 + 16x^3 + 22x^2 + 16x + 8$$
$$=_5 x^7 + 2x^6 + 4x^5 + x^3 + 2x^2 + x + 3$$

5. $|\mathbb{Z}_2|^{3+1} = 2^4 = 16.$

6. $|\mathbb{Z}_5|^{2+1} = 5^3 = 225.$

7. $\phi_2(x^2+3) = 2^2 + 3 = 4 + 3 = 7 =_7 0.$

8. $\phi_0(2x^3 - x^2 + 3x + 2) = 2 \cdot 0^3 - 0^2 + 3 \cdot 0^1 + 2 = 2 =_7 2.$

9. $$\phi_3\left(f[x]\cdot g[x]\right)\overset{\text{homomorphism}}{=}\phi_3 f[x]\cdot\phi_3 g[x]$$
$$=\phi_3\left(x^4+2x\right)\cdot\phi_3\left(x^3-3x^2+3\right)$$
$$=\left(3^4+2\cdot3\right)\cdot\left(3^3-3\cdot3^2+3\right)=\left(81+6\right)\cdot\left(27-27+3\right)$$
$$=_7 3\cdot3=9=_7 2$$

10. $$\phi_5\left(\left(x^3+2\right)\left(4x^2+3\right)\left(x^7+3x^2+1\right)\right)=\phi_5\left(x^3+2\right)\cdot\phi_5\left(4x^2+3\right)\cdot\phi_5\left(x^7+3x^2+1\right)$$
$$=\left(5^3+2\right)\cdot\left(4\cdot5^2+3\right)\cdot\left(5^7+3\cdot5^2+1\right)$$
$$=_5 127\cdot103\cdot\left(5+75+1\right)=_5 2\cdot3+1=6=_5 1$$

11. $$\phi_4\left(3x^{106}+5x^{99}+2x^{53}\right)=_4\phi_4\left(3x^4+5x^3+2x^5\right)$$
$$=3\cdot4^4+5\cdot4^3+2\cdot4^5=3\cdot256+5\cdot64+2\cdot1024$$
$$=_4 3\cdot0+5\cdot0+2\cdot0=0$$

12. $\phi_{(0,1)}\left(x^2+1\right)=\left(1,2\right)=_2=\left(1,0\right)\Rightarrow\operatorname{Ker}\left(x^2+1\right)=\left\{1\right\}$.

13. $\phi_{(0,\ldots,6)}\left(x^3+2x+2\right)=\left(2,5,14,35,74,137,230\right)=_7\left(2,5,0,0,4,4,6\right)\Rightarrow\operatorname{Ker}\left(x^3+2x+2\right)=\left\{2,3\right\}$.

14. $$\phi_{(0,\ldots,4)}\left(x^5+3x^3+x^2+2x\right)=\phi_{(0,\ldots,4)}\left(3x^3+x^2+3x\right)=\left(0,7,34,99,220\right)=_5\left(0,2,4,4,0\right)$$
$$\Rightarrow\operatorname{Ker}\left(3x^3+x^2+3x\right)=\left\{0,4\right\}$$

15. $$\phi_{(0,\ldots6)}\left(f[x]\cdot g[x]\right)=\left({}_{i\in(0,\ldots6)}\phi_i f[x]\cdot\phi_i g[x]\right)=\left(5\cdot0,8\cdot5,21\cdot16,50\cdot33,101\cdot56,230\cdot85,293\cdot110\right)$$
$$=_7\left(5\cdot0,1\cdot5,0\cdot2,1\cdot5,3\cdot0,6\cdot1,5\cdot5\right)$$
$$=\left(0,5,0,5,0,6,25\right)=_7\left(0,5,0,5,0,6,4\right)$$
$$\Rightarrow\operatorname{Ker}\left(f[x]\cdot g[x]\right)=\left\{0,2,4\right\}$$

16. $\phi_3\left(x^{231}+3x^{117}-2x^{53}+1\right)=_5\phi_3\left(x^3+3x^1-2x^1+1\right)=\phi_3\left(x^3+x+1\right)=27+3+1=31=_5 1$.

17. $$2x^{219}+3x^{74}+2x^{57}+3x^{44}=_5 2x^3+3x^2+2x^1+3x^0$$
$$\phi_{(0,\ldots,4)}\left(2x^3+3x^2+2x^1+3x^0\right)=\left(0,10,35,90,187\right)=_5\left(0,0,0,0,2\right)$$
$$\operatorname{Ker}\left(2x^{219}+3x^{74}+2x^{57}+3x^{44}\right)=\left\{0,1,2,3\right\}$$

18. Replace "coefficients a_i" and "$a_i\neq0$ for a finite number of *i*".

19. Seems okay.

20. $$\left(3x^3+2x\right)y^3+\left(x^2-6x+1\right)y^2+\left(x^4-2x\right)y+\left(x^4-3x^2+2\right)$$
$$=3x^3y^3+2xy^3+x^2y^2-6xy^2+y^2+x^4y-2xy+x^4-3x^2+2$$
$$=\left(y+1\right)x^4+\left(3y^3\right)x^3+\left(y^2-3\right)x^2+\left(2y^3-6y^2-2y\right)x+\left(y^2+2\right)$$

21. $\left\{{}_{i\in\mathbb{N}}\,\frac{1}{5}x^{i+1}-x^i\right\}\subseteq\operatorname{Ker}\phi_5:\mathbb{Q}[x]\to\mathbb{R}$.

22. 1 is unity in $\mathbb{Z}_4\Rightarrow 1$ is unity in $\mathbb{Z}_4[x]$. $1+2x\in\mathbb{Z}_4[x]$ has $\left(1+2x\right)^{-1}=1-2x$.

23. a. true

b. true (Theorem 2)

c. true (If *D* has no divisors of zero, then $D[x]$ cannot possibly have them either)

d. true (if $d\in D$ is a divisor of zero with $d'\in D: dd'=0$, then $dx\cdot d'x=0x^2=0$)

e. false

f. false ($2x^3 \cdot 2x^4 =_{\mathbb{Z}_4[x]} 4x^7 = 0$)

g. true (because $\phi_\alpha\big(f[x]g[x]\big) = \phi_a f[x] \cdot \phi_\alpha g[x] = 0 \cdot \phi_a g[x] = 0$)

h. true (if F is a field it has no divisors of zero, so a product with a polynomial of degree > 0 can never have degree 0)

i. true (because $1 \in R$ is never a divisor of zero)

j. false ($2x \in \mathbb{Z}_4[x]$ is a divisor of zero, because $2x \cdot 2x = 4x^2 = 0$)

24. Theorem 2 says that if F is a commutative ring then $F[x]$ is also. Remaining to be proved that if D has no divisors of zero, neither does $D[x]$. $\forall f[x] \in D[x], f[x] \neq 0 \Rightarrow f[x] = +_{i\in\mathbb{N}} f_i x^i : \exists i \in \mathbb{N} \vdots a_i \neq 0$. For any $g \in D[x], g[x] = +_{i\in\mathbb{N}} g_i x^i$, let f_i, g_i be the first coefficients of $f[x], g[x]$ such that $f_i, g_j \neq 0$. Since D is an integral domain, $f_i g_j \neq 0$, and since this the only term of degree $i+j$ of $f[x] \cdot g[x], f[x] \cdot g[x] \neq 0$.

25. a. Since an integral domain has no divisors of zero, suppose $f[x]$ is of degree ≥ 1 and $f[x] = +_i f_i x^i$, $g[x] = +_i g_i x^i$, let f_i, g_j be the highest coefficients $f_i \neq 0, g_j \neq 0; i, j \geq 1$. Then $f[x] \cdot g[x]$ will contain a term $f_i g_j \neq 0 \Rightarrow f[x] \cdot g[x] \neq 1$. For every $f[x]$ of degree 0 $f[x] = f_0$, so $f[x] \cdot g[x] = 1[x]$ iff $f_0 \in D$ is a unit. If the degree of $f[x] \ngeq 0$, then $f[x] = 0 \Rightarrow f[x] \cdot g[x] \neq 1[x]$. So the units of $D[x]$ are exactly the units of D.

b. The only units of $\mathbb{Z}$ are 1 and –1, so by (a.) $1[x], -1[x]$ are the only units of $\mathbb{Z}[x]$.

c. By Corollary 2.12, $\mathbb{Z}_7$ is a field so all $i \in \mathbb{Z}_7^{\,*}$ are units, so by (a.) all $\left\{_{i\in\mathbb{Z}_7^{\,*}} i[x]\right\}$ are units.

26. $\forall f[x], g[x], h[x] \in R[x]$:

$$f[x] \cdot \big(g[x] \cdot h[x]\big) = +_i f_i x^i \left(+_i g_i x^i + +_i h_i x^i\right)$$

$$\overset{\text{definition}}{=} \quad +_i f_i x^i \cdot +_i \left(g_i + h_i\right) x^i$$

$$\overset{\text{definition}}{=} \quad +_i \left(+_{j=0}^{i} f_j \left(g_{i-j} h_{i-j}\right)\right) x^i$$

$$\overset{\text{Def 5.1R3}}{=} \quad +_i \left(+_{j=0}^{i} f_j g_{i-j} + +_{j=0}^{i} f_j h_{i-j}\right) x^i$$

$$= +_i\left(\left(+_{j=0}^{i} f_j g_{i-j}\right) x^i + \left(+_{j=0}^{i} f_j h_{i-j}\right) x^i\right)$$

$$= +_i \left(+_{j=0}^{i} f_j g_{i-j}\right) x^i + +_i \left(+_{j=0}^{i} f_j h_{i-j}\right) x^i$$

$$\overset{\text{definition}}{=} \quad +_i f_i x^i \cdot +_i g_i x^i + +_i f_i x^i \cdot +_i h_i x^i$$

$$= f[x] \cdot g[x] + f[x] \cdot h[x]$$

27. a. $\forall f[x], g[x] \in F[x]$:

$$D\big(f[x] + g[x]\big) = D\left(+_i f_i x^i + +_i g_i x^i\right) = D +_i \left(f_i + g_i\right) x^i$$

$$= +_{i+1} i \cdot \left(f_i + g_i\right) x^{i-1} \overset{\text{5.1R3}}{=} +_{i+1} \left(i \cdot f_i + i \cdot g_i\right) x^{i-1}$$

$$\overset{\text{definition}}{=} \quad +_{i+1} \left(i \cdot f_i\right) x^{i-1} + +_i \left(i \cdot g_i\right) x^{i-1} = D +_i f_i x^i + D +_i g_i x^i$$

$$= Df[x] + Dg[x]$$

So D is a group homomorphism. But $Dx \cdot Dx = 1 \cdot 1 = 0 \neq Dx^2 = 2x$, so D is not a ring homomorphism.

b. $\forall f[x] \in F[x] : Df[x] = 0 \Rightarrow D +_i f_i x^i = +_{i+1} i f_i x^{i-1} = 0 \Leftrightarrow \forall i > 0 : f_i = 0$, so $\operatorname{Ker} D = \left\{_{f_0 \in F} f_0 x^0\right\} = F$.

c. $(\Rightarrow)\ \forall f\left[x\right]\in F\left[x\right]: Df\left[x\right]=D+_i f_i x^i=+_{i\geq 1} i f_i x^{i-1}\in F\left[x\right]$

$(\Leftarrow)\ \forall f\left[x\right]\in F\left[x\right]: f\left[x\right]=+_i f_i x^i : D+_i \dfrac{f_i}{i+1}x^{i+1}=+_{i\geq 1} i\dfrac{f_{i-1}}{i}x^{i-1}=+_{i\geq 1} f_{i-1}x^{i-1}=+_i f_i x^i=f\left[x\right]$.

28. a. $\phi_{\left({}^{n}_{i}\alpha_i\in E\right)}: F\left[{}^{n}_{i}x_i\right]\to E: f\left[{}^{n}_{i}x_i\right]=+_{\left({}^{n}_{i}p_i\right)}f_{\left({}^{n}_{i}p_i\right)}\cdot^{n}_{i}x_i^{p_i}\mapsto +_{\left({}^{n}_{i}p_i\right)}f_{\left({}^{n}_{i}p_i\right)}\cdot^{n}_{i}\alpha_i^{p_i}$.

b. $\phi_{-3,2}\left(x_1^{\ 2}x_2^{\ 2}+3x_1^{\ 4}x_2\right)=\left(-3\right)^2\cdot 2^2+3\cdot\left(-3\right)^4\cdot 2^1=9\cdot 4+3\cdot 81\cdot 2=36+486=519$.

c. A zero of a polynomial $f\left[{}^{n}_{i}x_i\right]$ is an n-tuple $\left({}^{n}_{i}\alpha_i\right)$ such that $\phi_{\left({}^{n}_{i}\alpha_i\right)}f\left[{}^{n}_{i}\alpha_i\right]=0$.

29. $R^R=\left\{{}_{f:R\to R}f\right\}$.

- (associativity) $\forall\phi,\psi,\varphi\in R^R,\forall r\in R$: $\left(\left(\phi+\psi\right)+\varphi\right)r=\left(\phi+\psi\right)r+\varphi r=\phi r+\psi y+\varphi r=\phi r+\left(\psi+\varphi\right)r=\left(\phi+\left(\psi+\varphi\right)\right)r$.
- (additive identity) $0\in R^R: r\mapsto 0;\quad \forall\phi\in R^R:\left(\phi+0\right)r=\phi r+0r=\phi r$.
- (additive inverse) $\forall\phi\in R^R:\exists\phi^{-1}\in R^R:\forall r\in R: r\mapsto -\phi r\Rightarrow\left(\phi+\phi^{-1}\right)r=\phi r+\phi^{-1}r=\phi r+\left(-\phi r\right)=0$.
- (multiplicative associativity) $\forall\phi,\psi,\varphi\in R^R:\forall r\in R$:
  $\left(\left(\phi\cdot\psi\right)\cdot\varphi\right)r=\left(\phi\cdot\psi\right)r\cdot\varphi r=\phi r\cdot\psi r\cdot\varphi r=\phi r\cdot\left(\psi\cdot\varphi\right)r=\left(\phi\cdot\left(\psi\cdot\varphi\right)\right)r$
- (left distributivity) $\forall\phi,\psi,\varphi\in R^R:\forall r\in R$:
  $\left(\phi\cdot\left(\psi+\varphi\right)\right)r=\phi r\cdot\left(\psi+\varphi\right)r=\phi r\cdot\left(\psi r+\varphi r\right)\overset{R\text{ a ring}}{=}\phi r\cdot\psi r+\phi r\cdot\varphi r=\left(\phi\cdot\psi\right)r+\left(\phi\cdot\varphi\right)r=\left(\phi\cdot\psi+\phi\cdot\varphi\right)r$
- (right distributivity) id.

30.
- (additive closure) $\forall\phi,\psi\in P_F:\phi\psi\overset{\text{Ex. 29}}{\in}P_F,\quad \exists f,g\in F\left[x\right]:\forall a\in F:\phi a=fa,\psi a=ga$
  $\forall a\in F:\left(\phi\psi\right)a=\phi a\cdot\psi a=fa\cdot ga=\left(f\cdot g\right)a\Rightarrow\phi\psi\in P_F$.
- (additive identity) $0_{F^F}\in F^F: a\mapsto 0.\ \ 0_{P_F}\in P_F:+_i 0\cdot x^i: a\mapsto 0\quad\Rightarrow 0_{P_F}=0_{F^F}$.
- (additive inverse) $\forall\phi\in P_F:\exists f\left[x\right]\in F\left[x\right]:\forall a\in F:\phi a=f\left[x\right]a$:
  $\phi^{-1}\in F^F:\forall a\in F:\phi^{-1}a=-\phi a\quad\Rightarrow\forall a\in F:\left(\phi+\phi^{-1}\right)a=\phi a+\phi^{-1}a=\phi a+\left(-\phi a\right)=0$
  $\Rightarrow f^{-1}\in F\left[x\right]:\forall a\in F:f^{-1}a=-fa\Rightarrow\forall a\in F:\phi a=fa\Rightarrow\phi^{-1}\in P_F$
- (multiplicative closure) $\forall\phi,\psi\in P_F:\exists f,g\in F\left[x\right]:\forall a\in F:\phi a=fa,\psi a=ga$
  $\Rightarrow\forall a\in F:\left(\phi\cdot\psi\right)a=\phi a\cdot\psi a=\left(f\cdot g\right)a, f\cdot g\in F\left[x\right]\Rightarrow\phi\cdot\psi\in P_F$.
- (left, right distributivity) …

b. It seems obvious that every polynomial can be interpreted as an element of P_F under the evaluation homomorphism, and conversely. So they can be not isomorphic only considering 'tricks' such as letting x^2 and $\left(-x\right)^2$ be 'different functions' in F^F.

31. a. $\left|\mathbb{Z}_2^{\ \mathbb{Z}_2}\right|=\left|\mathbb{Z}_2\right|^{\left|\mathbb{Z}_2\right|}=2^2=4;\ \left|\mathbb{Z}_3^{\ \mathbb{Z}_3}\right|=\left|\mathbb{Z}_3\right|^{\left|\mathbb{Z}_3\right|}=3^3=27$.

b. $\left\langle\mathbb{Z}_2^{\ \mathbb{Z}_2},+\right\rangle\cong\mathbb{Z}_2\times\mathbb{Z}_2;\ \left\langle\mathbb{Z}_3^{\ \mathbb{Z}_3},+\right\rangle\cong\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3$.

c. It remains to be shown that $\forall\varphi\in F^F\Rightarrow\varphi\in P_F$.

$f_i\left[x\right]\in F\left[x\right]:\alpha\mapsto\left(\alpha-a_1\right)\left(\alpha-a_2\right)\ldots\left(\alpha-a_{i-1}\right)\left(\alpha-a_{i+1}\right)\ldots\left(\alpha-a_{|F|}\right)$ so that

$$\begin{cases} \alpha \neq a_i : f_i[x]\alpha = 0 \\ \alpha = a_i : f_i[x]\alpha = (a_i - a_1)(a_i - a_2)\ldots(a_i - a_{i-1})(a_i - a_{i+1})\ldots(a_i - a_{|F|}) \end{cases}$$

Let $f \in F[x] : \alpha \mapsto +_i^{|F|} \varphi x_i \dfrac{f_i[x]\alpha}{f_i[x]\alpha_i}$ (exists because F is a field), so

$\forall a_i \in F : fa_i = +_j^{|F|} \varphi a_j \dfrac{f_j[x]a_i}{f_j[x]a_j} = \varphi a_i \dfrac{f_i[x]a_i}{f_i[x]a_i} = \varphi a_i$ and $f \in P_F \Rightarrow F^F \subseteq P_F \Rightarrow F^F = P_F$.

§5.6 Factorization of Polynomials over a Field

♥1. Let $f[x] = +_i^n f_i x^i,\ g[x] = +_i^m g_i x^i \in F[x];\quad f_n, g_m \neq 0$. Then $f[x] = q[x]g[x] + r[x]$, where $q[x], r[x] \in F[x]$ are unique and $r[x] = 0 \vee \deg r[x] < \deg g[x]$. Roughly:

$$\frac{f[x]}{g[x]} = q[x] + \frac{r[x]}{g[x]}$$

1.
$$\begin{array}{l}
x^2 + 2x - 3 \;\big)\; x^6 + 3x^5 + 4x^2 - 3x + 2 \;\big(\; x^4 + x^3 + x^2 + x + 5 \\
\underline{x^6 + 2x^5 - 3x^4} \\
x^5 + 3x^4 + 4x^2 - 3x + 2 \\
\underline{x^5 + 2x^4 - 3x^3} \\
x^4 + 3x^3 + 4x^2 - 3x + 2 \\
\underline{x^4 + 2x^3 - 3x^2} \\
x^3 + 7x^2 - 3x + 2 \\
\underline{x^3 + 2x^2 - 3x} \\
5x^2 + 2 \\
\underline{5x^2 + 10x - 15} \\
-10x + 17 = 4x + 3
\end{array}$$

2.
$$\begin{array}{l}
3x^2 + 2x - 3 \;\big)\; x^6 + 3x^5 + 4x^2 - 3x + 2 \;\big(\; 5x^4 + 5x^2 + 6x \\
\underline{x^6 + 3x^5 + 6x^4} \\
x^4 + 4x^2 - 3x + 2 \\
\underline{x^4 + 3x^3 + 6x^2} \\
4x^3 + 5x^2 - 3x + 2 \\
\underline{4x^3 + 5x^2 + 3x} \\
x + 2
\end{array}$$

3.
$$\begin{array}{l}
2x + 1 \;\big)\; x^5 - 2x^4 + 3x - 5 \;\big(\; 6x^4 + 7x^3 + 2x^2 + 10x + 2 \\
\underline{x^5 + 6x^4} \\
3x^4 + 3x - 5 \\
\underline{3x^4 + 7x^3} \\
4x^3 + 3x - 5 \\
\underline{4x^3 + 2x^2} \\
9x^2 + 3x - 5 \\
\underline{9x^2 + 10x} \\
4x - 5 \\
\underline{4x + 2} \\
4
\end{array}$$

4. $$\begin{array}{lll} 5x^2 - x + 2 & \big/\ x^4 + 5x^3 - 3x^2\ \big\backslash & 9x^2 + 5x + 10 \\ & \underline{x^4 + 2x^3 + 7x^2} & \\ & \quad 3x^3 + x^2 & \\ & \quad \underline{3x^3 + 6x^2 + 10x} & \\ & \qquad 6x^2 + x & \\ & \qquad \underline{6x^2 + x + 9} & \\ & \qquad\qquad 2 & \end{array}$$

5. $\langle 2\rangle =_5 \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3\} = \mathbb{Z}_5^{\,*}$, so $\mathbb{Z}_5^{\,*} = \langle 2^1 =_5 2\rangle = \langle 2^3 =_5 3\rangle$; $\{2,3\}$.

6. $\langle 3\rangle =_7 \{3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5\} = \mathbb{Z}_7^{\,*}$, so $\mathbb{Z}_7^{\,*} = \langle 3^1 =_7 3\rangle = \langle 3^5 =_7 5\rangle$; $\{3,5\}$.

7. $\langle 3\rangle =_{17} \{3^0 =_{17} 1, 3^1 =_{17} 3, 3^2 =_{17} 9, 3^3 =_{17} 10, 3^4 =_{17} 13, 3^5 =_{17} 5, 3^6 =_{17} 15, 3^7 =_{17} 11,$, so

$3^8 =_{17} 16, 3^9 =_{17} 14, 3^{10} =_{17} 8, 3^{11} =_{17} 7, 3^{12} =_{17} 4, 3^{13} =_{17} 12, 3^{14} =_{17} 2, 3^{15} =_{17} 6\} = \mathbb{Z}_{17}^{\,*}$

$\mathbb{Z}_{17}^{\,*} = \langle 3^1 =_{17} 3\rangle, \langle 3^3 =_{17} 10\rangle, \langle 3^5 =_{17} 5\rangle, \langle 3^7 =_{17} 11\rangle, \langle 3^9 =_{17} 14\rangle, \langle 3^{11} =_{17} 7\rangle, \langle 3^{13} =_{17} 12\rangle, \langle 3^{15} =_{17} 6\rangle$;

$\{3,10,5,11,14,7,12,6\}$.

8. $\langle 5\rangle =_{23} \{5^0 =_{23} 1, 5^1 =_{23} 5, 5^2 =_{23} 2, 5^3 =_{23} 10, 5^4 =_{23} 4, 5^5 =_{23} 20, 5^6 =_{23} 8, 5^7 =_{23} 17, 5^8 =_{23} 16,$

$5^9 =_{23} 11, 5^{10} =_{23} 9, 5^{11} =_{23} 22, 5^{12} =_{23} 18, 5^{13} =_{23} 21, 5^{14} =_{23} 13, 5^{15} =_{23} 19, 5^{16} =_{23} 3,$

$5^{17} =_{23} 15, 5^{18} =_{23} 6, 5^{19} =_{23} 7, 5^{20} =_{23} 12, 5^{21} =_{23} 14\}$

, so $\mathbb{Z}_{23}^{\,*} = \langle 5^1 =_{23} 5\rangle = \langle 5^3 =_{23} 15\rangle = \langle 5^5 =_{23} 20\rangle = \langle 5^7 =_{23} 17\rangle = \langle 5^9 =_{23} 11\rangle$;

$= \langle 5^{13} =_{23} 21\rangle = \langle 5^{15} =_{23} 19\rangle = \langle 5^{17} =_{23} 15\rangle = \langle 5^{19} =_{23} 7\rangle = \langle 5^{21} =_{23} 14\rangle$

$\{5,10,20,17,11,21,19,15,7,14\}$.

9. $\phi_1\left(x^4 + 4\right) =_5 0;\quad \dfrac{x^4 + 4}{x - 1} = x^3 + x^2 + x + 1$

$\phi_2\left(x^3 + x^2 + x + 1\right) =_5 3 + 4 + 2 + 1 =_5 0;\quad \dfrac{x^3 + x^2 + x + 1}{x - 2} = x^2 + 3x + 2$

$\phi_3\left(x^2 + 3x + 2\right) =_5 4 + 4 + 2 =_5 0;\quad \dfrac{x^2 + 3x + 2}{x - 3} = x + 1$

$\Rightarrow x^4 + 4 =_5 (x - 1)(x - 2)(x - 3)(x - 4)$

10. $\phi_{-1}\left(x^3 + 2x^2 + 2x + 1\right) =_7 -1 + 2 = 2 + 1 =_7 0;\quad \dfrac{x^3 + 2x^2 + 2x + 1}{x + 1} = x^2 + x + 1$

$\phi_2\left(x^2 + x + 1\right) =_7 4 + 2 + 1 =_7 0;\quad \dfrac{x^2 + x + 1}{x - 2} = x + 3$

$\Rightarrow x^3 + 2x^2 + 2x + 1 =_7 (x + 1)(x - 2)(x + 3)$

11. $\phi_3\left(2x^3 + 3x^2 - 7x - 5\right) =_{11} -1 + 5 + 1 - 5 =_{11} 0;\quad \dfrac{2x^3 + 3x^2 - 7x - 5}{x - 3} = 2x^2 + 9x + 9$

$\phi_{-3}\left(2x^2 + 9x + 9\right) =_{11} 18 - 27 + 9 =_{11} 0;\quad \dfrac{2x^2 + 9x + 9}{x + 3} = 2x + 3$

$\phi_4\left(2x + 3\right) =_{11} 8 + 3 =_{11} 0;\quad \dfrac{2x + 3}{x - 4} = 2$

$\Rightarrow 2x^3 + 3x^2 - 7x - 5 =_{11} 2(x - 3)(x + 3)(x - 4)$

12. $\phi_2\left(x^3+2x+3\right)=_5 3+4+3=_5 0;\quad \dfrac{x^3+2x+3}{x-2}=x^2+2x+1$

$\phi_{-1}\left(x^2+2x+1\right)=_5 1-2+1=_5 0;\quad \dfrac{x^2+2x+1}{x+1}=x+1$

$\Rightarrow x^3+2x+3=_5 \left(x-2\right)\left(x+1\right)^2$

13. $\phi_{(0,\ldots,4)}\left(2x^3+x^2+2x+2\right)=_5 \left(2,2,1,1,4\right)$ is irreducible.

14. If $f\left[x\right]$ is reducible over $\mathbb{Q}$, then by Theorem 10 it has a zero in $\mathbb{Q}$, and by Corollary 12 it has a zero in $\mathbb{Z}$ that divides –2, which should therefore be one of $\left\{\pm1,\pm2\right\}$. But $\phi_{\{\pm1,\pm2\}}f\left[x\right]=\left\{7,-9,18,-16\right\}$. The roots of $f\left[x\right]$ are $\dfrac{-8\pm\sqrt{8^2-4\cdot1\cdot-2}}{2\cdot1}=-4\pm\frac{1}{2}\sqrt{64+8}$, so $f\left[x\right]$ is reducible over $\mathbb{R}$ and $\mathbb{C}$.

15. $g\left[x\right]$ is an Eisenstein polynomial with $p=3$, so it is irreducible over $\mathbb{Q}$. Since $D=\sqrt{6^2-4\cdot1\cdot12}=\sqrt{36-48}$ it is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.

16. By Corollary 12, if it is reducible over $\mathbb{Q}$ then it has a zero in $\mathbb{Z}$ that divides –8, which should therefore be one of $\left\{\pm1,\pm2,\pm4\right\}$. But $\phi_{\{\pm1,\pm2,\pm4\}}\left(x^3+3x^2-8\right)=\left\{-4,-6,12,-4,104,-24\right\}$.

17. Likewise, it should have a zero that divides 1, which should therefore itself be 1. But $\phi_{\{\pm1\}}\left(x^4-22x^2+1\right)=\left\{-20,-22\right\}$.

18. Yes for $p=3$, $a_2=1\neq_3 0$, $a_1=_3 0$, $a_0=-12\neq_{3^2} 0$.

19. Yes for $p=3$, $a_3=8\neq_3 0$, $a_2=6=_3 0$, $a_1=-9=_3 0$, $a_0=24\neq_{3^2} 0$.

20. No. Because $a_3=-9=-3^2$, the only possibility is $p=3$, but $a_0=-18=_{3^2} 0$.

21. Yes for $p=5$, $a_{10}=2\neq_5 0$, $a_3=-25=_5 0$, $a_2=10=_5 0$, $a_0=-30\neq_{5^2} 0$.

22. $x\in\left\{-\frac{5}{2},\frac{2}{3},\ldots\right\}$

$$\frac{6x^4+17x^3+7x^2+x-10}{x+\frac{5}{2}}=6x^3+2x^2+2x-4$$

$$\frac{6x^3+2x^2+2x-4}{x-\frac{2}{3}}=6x^2+6x+6$$

$6x^2+6x+6=0\Rightarrow\quad x^2+x+1=0;\quad \sqrt{1^2-4\cdot1\cdot1}=\sqrt{-3}$, so there are no other roots in $\mathbb{Q}$.

23. "nonconstant polynomial." Insert "and *g*, *h* both of lower degree than *f*."

24.

25. a. true (of degree 1, so both factors can't have degree less than 1)

b. true (same reason)

c. true (both roots are in $\mathbb{R}\setminus\mathbb{Q}$)

d. false (because 2 is a zero, so by Theorem 10 is reducible)

e. true (The degree of a product of nonzero polynomials is always the sum of the degrees of the factors, so a nonzero polynomial can only have an inverse if it is of degree 1. The zero polynomial has no inverse.)

f. ? (what is $F\left(x\right)$?)

g. true (Corollary 3)

h. true (Corollary 3)

i. true

j. false (because of the zero polynomial; however, the book gives "true")

26. $x+2$ is a factor if –2 is a zero, so

$\phi_{-2}\left(x^4+x^3+x^2-x+1\right)=0\Rightarrow\quad \left(-2\right)^4+\left(-2\right)^3+\left(-2\right)^2-\left(-2\right)+1=16-8+4+2+1=14=_p 0$, so $p\in\left\{2,7\right\}$.

27. x^2+x+1.

28. $x^3+x^2+1, \quad x^3+x+1$.

29. $x^2+1 \qquad 2x^2+2$
$x^2+x+2 \qquad 2x^2+x+1$
$x^2+2x+2 \qquad 2x^2+2x+1$

30. $x^3+2x+1 \qquad 2x^3+x+2$
$x^3+2x+2 \qquad 2x^3+x+1$
$x^3+x^2+2 \qquad 2x^3+2x^2+1$
$x^3+x^2+x+2 \qquad 2x^3+2x^2+2x+1$
$x^3+x^2+2x+1 \qquad 2x^3+2x^2+x+2$
$x^3+2x^2+1 \qquad 2x^3+x^2+2$
$x^3+2x^2+x+1 \qquad 2x^3+x^2+2x+2$
$x^3+2x^2+2x+2 \qquad 2x^3+x^2+x+1$

31.

32. By Euler's Theorem, $x^{p-1} =_p 1 \Rightarrow \quad x^p + a =_p x + a$. Thus, for any $a \in \mathbb{Z}_p$, $-a$ is a zero of $x^p + a$ so by the Factor Theorem $x + a$ is a factor of $x^p + a$, so it is not irreducible.

33. $a^n \cdot \phi_{1/a}\left(+_{i=0}^{n} a_{n-i} x^i\right) = a^n \cdot +_{i=0}^{n} a_{n-i} a^{-i} = +_{i=0}^{n} a_{n-i} a^{n-i} = +_{i=0}^{n} a_i a^i = \phi_a\left(a_i x^i\right) = 0 \overset{a \neq 0}{\Rightarrow} \quad \phi_{1/a}\left(+_{i=0}^{n} a_{n-i} x^i\right) = 0$.

34. $f[x] = q[x] \cdot (x - \alpha) + r[x]$. Then obviously, for $x = \alpha$: $f\alpha = q\alpha \cdot (\alpha - \alpha) + r\alpha = r\alpha$.

35. a. $\bar{\sigma}_m : \mathbb{Z}[x] \to \mathbb{Z}_m[x] : +_i a_i x^i \mapsto +_i \sigma_m a_i \cdot x^i$. For any $f[x] = +_i f_i x^i, g[x] = +_i g_i x^i \in \mathbb{Z}[x]$:

$$\bar{\sigma}_m\left(f[x] \cdot g[x]\right) = \bar{\sigma}_m\left(+_i f_i x^i \cdot +_i g_i x^i\right) = \bar{\sigma}_m\left(+_i +_j^i f_j g_{i-j} x^j\right) = +_i \sigma_m\left(+_j^i f_j g_{i-j}\right) x^i$$
$$=_m +_i\left(+_j^i \sigma_m f_i g_{i-j}\right) x^i =_m +_i\left(+_j^i \sigma_m f_i \cdot \sigma_m g_{i-j}\right) x^i = +_i \sigma_m f_i x^i \cdot +_i \sigma_m g_i x^i = \bar{\sigma}_m +_i f_i x^i \cdot \bar{\sigma}_m +_i g_i x^i$$
$$= \bar{\sigma}_m f[x] \cdot \bar{\sigma}_m g[x]$$

b. $\forall f[x] \in \mathbb{Z}[x]: \quad \deg f[x] = \deg \bar{\sigma}_m f[x]$. Suppose $\bar{\sigma}_m f[x] = g'[x] \cdot h'[x], \quad \deg g'[x], \deg h'[x] < \deg \bar{\sigma}_m f[x]$. Since $\bar{\sigma}_m$ is a homomorphism, $\exists g[x], h[x] \in \mathbb{Z}[x]$: $\bar{\sigma}_m g[x] = g'[x], \bar{\sigma}_m h[x] = h'[x]$, so

$\bar{\sigma}_m f[x] = \bar{\sigma}_m g[x] \cdot \bar{\sigma}_m h[x] \overset{\text{homomorphism}}{=} \bar{\sigma}_m g[x] h[x]$. Suppose $f[x]$ is reducible in $\mathbb{Z}[x]$ and by Theorem 11 then in $\mathbb{Q}[x]$ as $f[x] = g[x] \cdot h[x]$. Then $\bar{\sigma}_m f[x] = \bar{\sigma}_m g[x] h[x] = \bar{\sigma}_m g[x] \cdot \bar{\sigma}_m h[x]$ would also be reducible in $\mathbb{Z}_m[x]$ ($\bar{\sigma}_m$ does not affect the degree).

c. Consider $\bar{\sigma}_3\left(x^3 + 17x + 36\right) = x^3 + 2x = x\left(x^2 + 2\right) \ldots$

§5.7 Noncommutative Examples

1. $(2e + 3a + 0b) + (4e + 2a + 3b) = 1e + 0a + 3b$.

2. $(2e + 3a + 0b)(4e + 2a + 3b) = (2 \cdot 4 + 3 \cdot 3 + 0 \cdot 2)e + (2 \cdot 2 + 3 \cdot 4 + 0 \cdot 3)a + (2 \cdot 3 + 3 \cdot 2 + 0 \cdot 3)b = 2e + 1a + 2b$.

3. $(3e + 3a + 3b)^2 = (3 \cdot 3 + 3 \cdot 3 + 3 \cdot 3)e + \ldots a + \ldots b = 2e + 2a + 2b$

$(3e + 3a + 3b)^4 = (2e + 2a + 2b)^2 = (2 \cdot 2 + 2 \cdot 2 + 2 \cdot 2)e + \ldots a + \ldots b = 2e + 2a + 2b$.

4. $(i + 3j)(4 + 2j - k) = (0 \cdot 4 - 1 \cdot 0 - 3 \cdot 2 - 0 \cdot -1) + (0 \cdot 0 + 1 \cdot 4 + 3 \cdot -1 - 0 \cdot 2)i$
$+ (0 \cdot 2 - 1 \cdot -1 + 3 \cdot 4 + 0 \cdot 0)j + (0 \cdot -1 + 1 \cdot 2 - 3 \cdot 0 + 0 \cdot 4)k = -6 + 1i + 13j + 2k$

5. $i^2 j^3 kji^5 = i^2 j^2 jkj\left(i^2\right)^2 i = -1 \cdot -1 \cdot jkj\left(-1\right)^2 i = jkji = i \cdot -k = j$.

6. $\left(i+j\right)^2 = i \cdot i + i \cdot j + j \cdot i + j \cdot j = -1 + k - k - 1 = -2 \Rightarrow \quad \left(i+j\right)^{-1} = \dfrac{1}{i+j} \cdot \dfrac{i+j}{i+j} = \dfrac{i+j}{-2} = \tfrac{1}{2}\left(i+j\right)$.

7. $\left(1+3i\right)\left(4j+3k\right) = 1 \cdot 4j + 1 \cdot 3k + 3i \cdot 4j + 3i \cdot 3k = 4j + 3k + 12k - 9j = -5j + 15k = 5\left(-j+3k\right)$

$\left(-j+5k\right)^2 = -j \cdot -j - j \cdot 3k + 3k \cdot -j + 3k \cdot 3k = -1 - 3i + 3i - 9 = -10$

$\Rightarrow \quad \left(\left(1+3i\right)\left(3j+3k\right)\right)^{-1} = \dfrac{1}{5\left(-j+5k\right)} = \tfrac{1}{5}\dfrac{1}{-j+3k} \cdot \dfrac{-j+3k}{-j+3k} = \tfrac{1}{5}\dfrac{-j+3k}{-10} = \tfrac{1}{50}\left(j-3k\right)$

8. $\left(0\rho_0 + 1\rho_1 + 0\rho_2 + 0\mu_1 + 1\mu_2 + 1\mu_3\right)\left(1\rho_0 + 1\rho_1 + 0\rho_2 + 1\mu_1 + 0\mu_2 + 1\mu_3\right)$

$= \left(0\rho_0 + 0\rho_1 + 0\rho_2 + 0\mu_1 + 0\mu_2 + 0\mu_3\right) + \left(1\rho_1 + 1\rho_2 + 0\rho_0 + 1\mu_3 + 0\mu_1 + 1\mu_2\right) + \left(0\rho_0 + 0\rho_1 + 0\rho_2 + 0\mu_1 + 0\mu_2 + 0\mu_3\right)$

$+ \left(0\rho_0 + 0\rho_1 + 0\rho_2 + 0\mu_1 + 0\mu_2 + 0\mu_3\right) + \left(1\mu_2 + 1\mu_3 + 0\mu_1 + 1\rho_2 + 0\rho_0 + 1\rho_1\right) + \left(1\mu_3 + 1\mu_1 + 0\mu_2 + 1\rho_1 + 0\rho_2 + 1\rho_0\right)$

$= 1\rho_0 + 1\rho_1 + 0\rho_2 + 1\mu_1 + 0\mu_2 + 1\mu_3$

9. $\mathbb{R} \subset \mathbb{H}$ is commutative, so $Z\mathbb{R} = \mathbb{R}$. Now consider $\mathbb{H} \setminus \mathbb{R}$, that is all the quaternions that are nonzero in at least one of *i*, *j*, or *k*. Considering just these three components, we can show that they form a group isomorphic with $\mathbb{R}^3$ under vector cross product: $\forall g, h \in \mathbb{H} \setminus \mathbb{R}$:

$$\begin{aligned}
\phi\left(gh\right) &= \phi\left(\left(g_i i \cdot g_j j \cdot g_k k\right) \cdot \left(h_i i \cdot h_j j \cdot h_k k\right)\right) \\
&= \phi\left(\left(-g_i h_i 1 + g_i h_j k - g_i h_k j\right) + \left(-g_j h_i k - g_j h_j 1 + g_j h_k i\right) + \left(g_k h_i j - g_k h_j i - g_k h_k 1\right)\right) \\
&= \phi\left(\left(\ldots\right)1 + \left(g_j h_k - g_k h_j\right)i + \left(-g_i h_k + g_k h_i\right)j + \left(g_i h_j - g_j h_i\right)k\right) \\
&= \begin{bmatrix} g_j h_k - g_k h_j & g_k h_i - g_i h_k & g_i h_j - g_j h_i \end{bmatrix} \\
&= \begin{bmatrix} g_i & g_j & g_k \end{bmatrix} \times \begin{bmatrix} h_i & h_j & h_k \end{bmatrix} \\
&= \phi g \cdot \phi h
\end{aligned}$$

This shows that for any $g \in \mathbb{H} \setminus \mathbb{R}$ we can find an *h* which is noncolinear under its vector interpretation. Since $\mathbf{g} \times \mathbf{h} \neq \mathbf{h} \times \mathbf{g}$ for $\mathbf{g}, \mathbf{h} \neq \mathbf{0}$ and not colinear, we have that for any $\begin{bmatrix} g_1 & g_i & g_j & g_k \end{bmatrix}$, $\begin{bmatrix} g_1 & h_i & h_j & h_k \end{bmatrix}$ will not commute. So $Z\left(\mathbb{H} \setminus \mathbb{R}\right) = E$, and $Z\mathbb{H}^* = \mathbb{R}^*$.

10. Let $\mathbb{H}_{1j}, \mathbb{H}_{1k} \subset \mathbb{H}$ such that $\mathbb{H}_{1j} = \left\{ {}_{h_i, h_k = 0} h_1 1 + h_i i + h_j j + h_k k \right\}$ and $\mathbb{H}_{1k} = \left\{ {}_{h_i, h_j = 0} h_1 1 + h_i i + h_j j + h_k k \right\}$. In the following, consider *j*, *k* as quaternions but let *i* be the complex root of -1. Show that the field of complex numbers is isomorphic to one of these subsets of the quaternions under a simple projection $\pi_{1j} : \mathbb{H}_{1j} \to \mathbb{C} : \left(h_1 1 + 0 i_{\mathbb{H}} + h_j j + 0k\right) \mapsto h_1 + h_j i$. Then $\forall g, h \in \mathbb{C} : g = g_1 + g_i i, \quad h = h_1 + h_i i$:

- $$\begin{aligned}
{\pi_{1j}}^{-1} g + {\pi_{1j}}^{-1} h &= {\pi_{1j}}^{-1}\left(g_1 + g_i i\right) + {\pi_{1j}}^{-1}\left(h_1 + h_i i\right) \\
&= \left(g_1 1 + 0i + g_i j + 0k\right) + \left(h_1 1 + 0i + h_i j + 0k\right) \\
&= \left(\left(g_1 + h_1\right)1 + 0i + \left(g_i + h_i\right)j + 0k\right) \\
&= {\pi_{1j}}^{-1}\left(\left(g_1 + h_1\right) + \left(g_i + h_i\right)i\right) = {\pi_{1j}}^{-1}\left(g + h\right)
\end{aligned}$$

- $$\begin{aligned}
{\pi_{1j}}^{-1} g \cdot {\pi_{1j}}^{-1} h &= {\pi_{1j}}^{-1}\left(g_1 + g_i i\right) \cdot {\pi_{1j}}^{-1}\left(h_1 + h_i i\right) \\
&= \left(g_1 1 + 0 g_i + g_i j + 0 g_k\right) \cdot \left(h_1 1 + 0 h_i + h_i j + 0 h_k\right) \\
&= \left(g_1 h_1 1 + g_1 h_i j + g_i h_1 j - g_i h_i 1\right) \\
&= \left(\left(g_1 h_1 - g_i h_i\right)1 + 0i + \left(g_1 h_i + g_i h_1\right)j + 0k\right) \\
&= {\pi_{1j}}^{-1}\left(\left(g_1 h_1 - g_i h_i\right) + \left(g_1 h_i + g_i h_1\right)i\right) = {\pi_{1j}}^{-1}\left(g \cdot h\right)
\end{aligned}$$

so π_{1j}^{-1} is a ring homomorphism. Obviously $\operatorname{Ker}\pi_{1j}^{-1} = 0_{\mathbb{C}}$ and $\pi_{1j}^{-1}\mathbb{C} = \mathbb{H}_{1j}$, so it is an isomorphism and $\mathbb{C} \cong \mathbb{H}_{1j}$. Similarly, $\mathbb{C} \cong \mathbb{H}_{1k}$. Obviously $\mathbb{H}_{1j} \neq \mathbb{H}_{1k}$.

11. a. false (Example 2.8)

b. false (for $\mathbf{A} \in \mathrm{M}_2\,\mathbb{Z}_2$ to have an inverse, $\left|\mathbf{A}\right| \neq 0$)

c. false ($\operatorname{End} E$ has only one element and can therefore not have a nonzero multiplicative identity)

d. false ($\operatorname{End}\mathbb{R}$ has nonzero multiplicative identity)

e. false (isomorphisms under addition are generally not again isomorphisms, e.g. $f : \mathbb{R} \to \mathbb{R} : x \mapsto -x$, $f - f = 0_{\mathbb{R}\to\mathbb{R}}$)

f. false ($R\left\langle \mathbb{Z}, + \right\rangle$ as a group ring has elements that are formal sums that can't be combined under $+_{\mathbb{Z}}$ and is therefore infinite-dimensional)

g. true (by the definition, $+_i a_i g_i \cdot +_i b_i g_i = +_i\left(+_{j,k,g_i : g_i = g_j g_k} a_j b_k\right)g_i = +_i\left(+_{j,k,g_i : g_i = g_j g_k} b_k a_j\right)g_i = +_i b_i g_i \cdot +_i a_i g_i$ iff R is commutative)

h. false ($\mathbb{H}$ is not commutative)

i. true ($\cdot_{\mathbb{H}^*}$ is associative by the definition of a ring, generates inverses because the field of quaternions is strictly skew by Theorem 9, and thus commutative with multiplicative identity 1 by definition; and thus meets all of the requirements for a group)

j. false ($\mathbb{R} \subset \mathbb{H}$ is a field)

12. a. In $\mathbb{H}$, $x^2 + 1 = 0$ has solutions $i^2 + 1 = 0$, $j^2 + 1 = 0$, $k^2 + 1 = 0$.

b. Consider the multiplicative subgroup of $\mathbb{H}$. This is indeed a group because it is associative by definition of a ring, and each element has an inverse because it is strictly skew. None of the elements of this group are generators: $\left(\pm 1\right)^2 = 1, \left(\pm i\right)^2 = -1, \left(\pm j\right)^2 = -1, \left(\pm k\right)^2 = -1$.

13. $\phi \in \operatorname{End}\left\langle \mathbb{Z} \times \mathbb{Z} \right\rangle : \phi\left(m, n\right) = \left(m + n, 0\right)$, and let $\chi \in \operatorname{End}\left\langle \mathbb{Z} \times \mathbb{Z} \right\rangle : \chi\left(m, n\right) = \left(m, -m\right)$. Then $\left(\phi\chi\right)\left(m, n\right) = \phi\left(\chi\left(m, n\right)\right) = \phi\left(m, -m\right) = m + \left(-m\right) = 0$, so ϕ is a left divisor also.

14. Since F is a field, $0, 1 \in F$. An element of $\mathrm{M}_2 F$ has a multiplicative inverse iff its determinant is nonzero, which includes $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

15. Characterize all the endomorphisms ϕ of $\mathbb{Z}$. First, $\phi 0 = 0$. Second, let $\phi 1 = n$, then $\phi i = n \cdot i$ and this fully determines ϕ. So $\phi_n, n \in \mathbb{Z}$ are all the endomorphisms. Also, if $n \in \mathbb{Z}^*$ then ϕ_n is an automorphism. Now consider the map $\psi : \operatorname{End}\mathbb{Z} \to \mathbb{Z} : \phi_n \mapsto n$. Then $\forall \phi_n, \phi_m \in \operatorname{End}\mathbb{Z}$ and $\forall i \in \mathbb{Z}$:

- $\phi_n i + \phi_m i = n \cdot i + m \cdot i = \left(n + m\right) \cdot i = \phi_{n+m} i \Rightarrow \quad \phi_n + \phi_m = \phi_{n+m} \Rightarrow \quad \psi\phi_n + \psi\phi_m = n + m = \psi\phi_{n+m} = \psi\left(\phi_n + \phi_m\right)$.
- $\left(\phi_n \cdot \phi_m\right)i = \phi_n\left(\phi_m i\right) = \phi_n\left(m \cdot i\right) = \left(n \cdot m\right) \cdot i = \phi_{n \cdot m} i \Rightarrow \quad \phi_n \cdot \phi_m = \phi_{n \cdot m} \Rightarrow \quad \psi\phi_n \cdot \psi\phi_m = n \cdot m = \psi\phi_{n \cdot m} = \psi\left(\phi_n \cdot \phi_m\right)$.

so ψ is a homomorphism. Furthermore, $\forall n \in \mathbb{Z}^* : \quad \exists \phi_n \in \operatorname{End}\mathbb{Z}$ so ψ is surjective, and $\operatorname{Ker}\psi = \phi_1$ so ψ is injective and bijective, so ψ is an isomorphism.

16.

17. $\forall +_i\, a_i x^i \in F\left[x\right]$:

$$\begin{aligned} \left(\Upsilon X - X\Upsilon\right)\left(+_i a_i x^i\right) &= \left(\Upsilon X\right)\left(+_i a_i x^i\right) - \left(X\Upsilon\right)\left(+_i a_i x^i\right) \\ &= \Upsilon\left(X\left(+_i a_i x^i\right)\right) - X\left(\Upsilon\left(+_i a_i x^i\right)\right) \\ &= \Upsilon\left(+_i a_i x^{i+1}\right) - X\left(+_i i a_i x^{i-1}\right) \\ &= +_i\left(i + 1\right)a_i x^i - +_i i a_i x^i = +_i a_i x^i \end{aligned}$$

so $\Upsilon X - X\Upsilon = 1$.

18. If $G = E = \left\{e\right\}$, then by definition $RE = \left\{_{r_e \in R}\, r_e e\right\}$. Let $\phi : RE \to R : r_e e \mapsto r_e$, then $\forall re, r'e \in RE$:

$\phi\left(re+r'e\right)=\phi\left(\left(r+r'\right)e\right)=r+r'=\phi\left(re\right)+\phi\left(r'e\right)$ and $\phi\left(re\cdot r'e\right)=\phi\left(\left(rr'\right)e\right)=rr'=\phi\left(re\right)\cdot\phi\left(r'e\right)$, so ϕ is a homomorphism. Since $\forall r\in R:\quad \exists re\in RE:\quad \phi rg=r$, ϕ is surjective and because $\phi\left(rg\right)=r=0_R \Rightarrow \quad rg=0_{RG}$ we have that $\operatorname{Ker}\phi=\left\{0_{RG}\right\}$ so ϕ is injective and bijective, so ϕ is an isomorphism and $RE\cong R$.

19. $\forall a,b,c\in\mathbb{H}:\quad a=a_1 1+a_i i+a_j j+a_k k,\ b=\ldots,\ c=\ldots:$

$$\begin{aligned}
\left(a\cdot b\right)c &=\left(\left(a_1 1+a_i i+a_j j+a_k k\right)\cdot\left(b_1 1+b_i i+b_j j+b_k k\right)\right)\cdot\left(c_1 1+c_i i+c_j j+c_k k\right)\\
&=\left(\left(a_1b_1\right)1+\left(a_1b_i\right)i+\left(a_1b_j\right)j+\left(a_1b_k\right)k+\left(a_ib_1\right)i-\left(a_ib_i\right)1+\left(a_ib_j\right)k-\left(a_ib_k\right)j\right.\\
&\quad\left.+\left(a_jb_1\right)j-\left(a_jb_i\right)k-\left(a_jb_j\right)1+\left(a_jb_k\right)i+\left(a_kb_1\right)k+\left(a_kb_i\right)j-\left(a_kb_j\right)i-\left(a_kb_k\right)1\right)\cdot\left(c_1 1+c_i i+c_j j+c_k k\right)\\
&=\left(\left(a_1b_1-a_ib_i-a_jb_j-a_kb_k\right)1+\left(a_1b_i+a_ib_1+a_jb_k-a_kb_j\right)i+\left(a_1b_j-a_ib_k+a_jb_i+a_kb_i\right)j+\left(a_1b_k+a_ib_j-a_jb_i+a_kb_1\right)k\right)\cdot\left(c_1 1+c_i i+c_j j+c_k k\right)\\
&=\left(a_1b_1-a_ib_i-a_jb_j-a_kb_k\right)c_1 1+\left(a_1b_1-a_ib_i-a_jb_j-a_kb_k\right)c_i i+\left(a_1b_1-a_ib_i-a_jb_j-a_kb_k\right)c_j j+\left(a_1b_1-a_ib_i-a_jb_j-a_kb_k\right)c_k k\\
&\quad+\left(a_1b_i+a_ib_1+a_jb_k-a_kb_j\right)c_1 i-\left(a_1b_i+a_ib_1+a_jb_k-a_kb_j\right)c_i 1+\left(a_1b_i+a_ib_1+a_jb_k-a_kb_j\right)c_j k-\left(a_1b_i+a_ib_1+a_jb_k-a_kb_j\right)c_k j\\
&\quad+\left(a_1b_j-a_ib_k+a_jb_1+a_kb_i\right)c_1 j-\left(a_1b_j-a_ib_k+a_jb_1+a_kb_i\right)c_i k-\left(a_1b_j-a_ib_k+a_jb_1+a_kb_i\right)c_j 1+\left(a_1b_j-a_ib_k+a_jb_1+a_kb_i\right)c_k i\\
&\quad+\left(a_1b_k+a_ib_j-a_jb_i+a_kb_1\right)c_1 k+\left(a_1b_k+a_ib_j-a_jb_i+a_kb_1\right)c_i j-\left(a_1b_k+a_ib_j-a_jb_i+a_kb_1\right)c_j i-\left(a_1b_k+a_ib_j-a_jb_i+a_kb_1\right)c_k 1\\
&=\left(a_1b_1c_1-a_ib_ic_1-a_jb_jc_1-a_kb_kc_1-a_1b_ic_i-a_ib_1c_i-a_jb_kc_i+a_kb_jc_i-a_1b_jc_j+a_ib_kc_j-a_jb_1c_j-a_kb_ic_j-a_1b_kc_k-a_ib_jc_k+a_jb_ic_k-a_kb_1c_k\right)1\\
&\quad+\left(a_1b_1c_i-a_ib_ic_i-a_jb_jc_i-a_kb_kc_i+a_1b_ic_1+a_ib_1c_1+a_jb_kc_1-a_kb_jc_1+a_1b_jc_k-a_ib_kc_k+a_jb_1c_k+a_kb_ic_k-a_1b_kc_j-a_ib_jc_j+a_jb_ic_j-a_kb_1c_j\right)i\\
&\quad+\left(a_1b_1c_j-a_ib_ic_j-a_jb_jc_j-a_kb_kc_j-a_1b_ic_k-a_ib_1c_k-a_jb_kc_k+a_kb_jc_k+a_1b_jc_1-a_ib_kc_1+a_jb_1c_1+a_kb_ic_1+a_1b_kc_i+a_ib_jc_i-a_jb_ic_i+a_kb_1c_i\right)j\\
&\quad+\left(a_1b_1c_k-a_ib_ic_k-a_jb_jc_k-a_kb_kc_k+a_1b_ic_j+a_ib_1c_j+a_jb_kc_j-a_kb_jc_j-a_1b_jc_i+a_ib_kc_i-a_jb_1c_i-a_kb_ic_i+a_1b_kc_1+a_ib_jc_1-a_jb_ic_1+a_kb_1c_1\right)k\\
&=a_1\left(b_1c_1-b_ic_i-b_jc_j-b_kc_k\right)1+a_i\left(-b_ic_i+b_1c_1-b_kc_k-b_jc_j\right)i+a_j\left(-b_jc_j-b_kc_k+b_1c_1-b_ic_i\right)j+a_k\left(-b_kc_k-b_jc_j-b_ic_i+b_1c_1\right)k\\
&\quad+a_1\left(b_1c_i+b_ic_1+b_jc_k-b_kc_j\right)i-a_i\left(b_ic_1+b_1c_i-b_kc_j+b_jc_k\right)1-a_j\left(b_jc_k-b_kc_j+b_1c_i+b_ic_1\right)k+a_k\left(-b_kc_j+b_jc_k+b_ic_1+b_1c_i\right)j\\
&\quad+a_1\left(b_1c_j-b_ic_k+b_jc_1+b_kc_i\right)j+a_i\left(-b_ic_k+b_1c_j+b_kc_i+b_jc_1\right)k-a_j\left(b_jc_1+b_kc_i+b_1c_j-b_ic_k\right)1-a_k\left(b_kc_i+b_jc_1-b_ic_k+b_1c_j\right)i\\
&\quad+a_1\left(b_1c_k+b_ic_j-b_jc_i+b_kc_1\right)k-a_i\left(b_ic_j+b_1c_k+b_kc_1-b_jc_i\right)j+a_j\left(-b_jc_i+b_kc_1+b_1c_k+b_ic_j\right)i-a_k\left(b_kc_1-b_jc_i+b_ic_j+b_1c_k\right)1\\
&=\left(a_1 1+a_i i+a_j j+a_k k\right)\cdot\left(\left(b_1c_1-b_ic_i-b_jc_j-b_kc_k\right)1+\left(b_1c_i+b_ic_1+b_jc_k-b_kc_j\right)i+\left(b_1c_j-b_ic_k+b_jc_1+b_kc_i\right)j+\left(b_1c_k+b_ic_j-b_jc_i+b_kc_1\right)k\right)\\
&=\left(a_1 1+a_i i+a_j j+a_k k\right)\cdot\quad\left(\left(b_1c_1\right)1+\left(b_1c_i\right)i+\left(b_1c_j\right)j+\left(b_1c_k\right)k+\left(b_1c_1\right)i-\left(b_ic_i\right)1+\left(b_ic_j\right)k-\left(b_ic_k\right)j\right.\\
&\qquad\qquad\left.+\left(b_jc_i\right)j-\left(b_jc_i\right)k-\left(b_jc_j\right)1+\left(b_jc_k\right)i+\left(b_kc_1\right)k+\left(b_kc_i\right)j-\left(b_kc_j\right)i-\left(b_kc_k\right)1\right)\\
&=\left(a_1 1+a_i i+a_j j+a_k k\right)\cdot\left(\left(b_1 1+b_i i+b_j j+b_k k\right)\cdot\left(c_1 1+c_i i+c_j j+c_k k\right)\right)=a\cdot\left(b\cdot c\right)
\end{aligned}$$

§5.8 Ordered Rings and Fields

1. $x-a\in P_{\text{high}} \Rightarrow \quad a<x;\quad x^2-x^1\in P_{\text{high}} \Rightarrow \quad x^1<x^2$; so $a<x^1<x^2<\ldots$.

2. $x^i-x^{i+1}\in P_{\text{low}} \Rightarrow \quad x^{i+1}<x^i$; so $\ldots x^3<x^2<x^1<x^0=1<x^{-1}<x^{-2}<x^{-3}\ldots$.

3. All the positive elements of $\mathbb{Z}\left[\sqrt{2}\right]$:

$$n+m\sqrt{2}\in P' \quad\Leftrightarrow\quad \phi^{\text{inv}}\left(n+m\sqrt{2}\right)\in P \quad\Leftrightarrow\quad n-m\sqrt{2}\in P \quad\Leftrightarrow\quad n-m\sqrt{2}>_{\mathbb{R}}0\Rightarrow \quad \vee\begin{cases} n>0\wedge m<0\\ n>0\wedge 2m^2<n^2\\ m>0\wedge n^2<2m^2\end{cases}.$$

4.	i. a c d e b	ii. d b a e c
5.	i. a c e d b	ii. e c b a d
6.	i. c a b e d	ii. e c a b d
7.	i. d a b c e	ii. d c e a b
8.	i. e a c b d	ii. c d a e b
9.	i. c a e d b	ii. e c b a d
10.	b d a c e	

11. a: $\dfrac{1}{1-x}=1+x+x^2+\ldots$; b: $\dfrac{x^2}{1+x}=x^2-x^3+x^4+\ldots$; c: $\dfrac{1}{x-x^2}=x^{-1}+1+x+\ldots$; d: $\dfrac{-x}{1+x^2}=-x+x^3-x^5+\ldots$;

e: $\dfrac{3-2x}{4x+x^3}=\tfrac{3}{4}x^{-1}-\tfrac{1}{2}+\ldots.$ d b a e c.

12. a: $\dfrac{5-7x}{x^2+3x^3}=5x^{-2}-22x^{-1}+\ldots;$ b: $\dfrac{-2+4x}{4-3x}=-\tfrac{1}{2}+\tfrac{5}{8}x+\ldots;$ c: $\dfrac{7+2x}{4-3x}=\tfrac{7}{4}+\ldots;$ d: $\dfrac{9-3x^2}{2+6x}=\tfrac{9}{2}+\ldots;$

e: $\dfrac{3-5x}{-6+2x}=-\tfrac{1}{2}+\tfrac{4}{6}x+\ldots.$ a b e c d.

13. a: $\dfrac{1-x}{1+x}=1-2x+\ldots;$ b: $\dfrac{3-5x}{3+5x}=1-\tfrac{10}{3}x+\ldots;$ c: $\dfrac{1}{4x+x^2}=\tfrac{1}{4}x^{-1}-\tfrac{1}{16}+\ldots;$ d: $\dfrac{1}{-3x+x^2}=-\tfrac{1}{3}x^{-1}-\tfrac{1}{9}+\ldots;$

e: $\dfrac{4x+x^2}{1-x}=4x+5x^2+\ldots.$ d e b a c.

14. The smallest subfield of the field of complex numbers containing $\sqrt[3]{2}$ is $\sqrt[3]{2}\subseteq\mathbb{R}$ and hence has the induced ordering from the field of real numbers. By Theorem 10, a subfield of $\mathbb{C}$ containing $\sqrt[3]{2}\cdot\dfrac{-1+i\sqrt{3}}{2}$ has an ordering induced from the isomorphism.

15. a. true (discussion after Example 2)
b. true (id.)
c. false (?)
d. true
e. true (both P_{low} and P_{high})
f. false (even in $\mathbb{R}$, if $a<0$ there is no such n)
g. true (if $b\le 0$ it's always true; if $b>0$ it's a restatement of Definition 7)
h. false ($-(-1)$ is positive)
i. false (neither $0,-0$ are positive)
j. true (Theorem 3)

16. With the ordering P_{high}, $\forall q\in\mathbb{Q}: q<\pi$.

17. $\forall m,n,m',n'\in\mathbb{Z}:\quad m+n\sqrt{2},m'+n'\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right]:$

$$\begin{aligned}\phi\left(\left(m+n\sqrt{2}\right)+\left(m'+n'\sqrt{2}\right)\right)&=\phi\left(\left(m+m'\right)+\left(n+n'\right)\sqrt{2}\right)\\&=\left(m+m'\right)-\left(n+n'\right)\sqrt{2}\\&=\left(m-n\sqrt{2}\right)+\left(m'-n'\sqrt{2}\right)\\&=\phi\left(m+n\sqrt{2}\right)+\phi\left(m'+n'\sqrt{2}\right)\end{aligned}$$

$$\begin{aligned}\phi\left(\left(m+n\sqrt{2}\right)\cdot\left(m'+n'\sqrt{2}\right)\right)&=\phi\left(\left(mm'+2nn'\right)+\left(mn'+m'n\right)\sqrt{2}\right)\\&=\left(mm'+2nn'\right)-\left(mn'+m'n\right)\sqrt{2}\\&=\left(m-n\sqrt{2}\right)\cdot\left(m'-n'\sqrt{2}\right)\\&=\phi\left(m+n\sqrt{2}\right)\cdot\phi\left(m'+n'\sqrt{2}\right)\end{aligned}$$

18. $a\in P\quad\Rightarrow a-0\in P\quad\overset{\text{Theorem 5}}{\Rightarrow}\quad 0<a.$

19. Lemma: $\forall a,c\in P; b\in R;\quad ab=c:\ \vee\begin{cases}b\in P: & a\cdot b\in P\quad\overset{\text{Definition 1}}{\Rightarrow}\quad c\in P\\ -b\in P: & a\cdot -b\in P\quad\Rightarrow -ab\in P\quad\Rightarrow -c\in P\,\text{(contradiction)}\\ b=0: & a\cdot b=0\notin P\quad\Rightarrow c\notin P\,\text{(contradiction)}\end{cases}\quad\Rightarrow b\in P.$

- $c = 0 \quad \Rightarrow ac = 0 \quad \Rightarrow bd = 0 \quad \overset{b\in P \Rightarrow b \neq 0}{\Rightarrow} \quad d = 0$.
- $c \in P \quad \Rightarrow ac \in P \quad \Rightarrow bd \in P \quad \overset{\text{Lemma}}{\Rightarrow} \quad d \in P \quad \Rightarrow cd \in P$.
- $-c \in P \quad \Rightarrow a \cdot (-c) \in P \quad \Rightarrow -(ac) \in P \quad \Rightarrow -(bd) \in P \quad \Rightarrow b \cdot (-d) \in P \quad \overset{\text{Lemma}}{\Rightarrow} \; -d \in P \quad \Rightarrow -c \cdot -d = c \cdot d \in P$.

20. $a < b \quad \Rightarrow b - a \in P \quad \Rightarrow -(-b) - a \in P \quad \Rightarrow (-a) - (-b) \in P \quad \Rightarrow -b < -a$.

21. $$\left.\begin{array}{lll} a < 0 & \Rightarrow 0 - a \in P & \Rightarrow -a \in P \\ 0 < b & \Rightarrow b - 0 \in P & \Rightarrow b \in P \end{array}\right\} \Rightarrow -ab \in P \quad \Rightarrow 0 - ab \in P \quad \Rightarrow ab < 0.$$

22. $b \cdot b^{-1} = 1;\ b, 1 \in P \quad \overset{\substack{\text{Lemma} \\ \text{from Ex.19}}}{\Rightarrow} \quad b^{-1} \in P; \quad a/b = ab^{-1} \quad \overset{\text{Definition 1}}{\in} \quad P$

23. $$\left.\begin{array}{lll} a < 1 & \Rightarrow 1 - a \in P & \\ 0 < a & \Rightarrow a - 0 = a \in P & \overset{\text{Lemma}}{\Rightarrow} \quad a^{-1} \in P \end{array}\right\} \Rightarrow a^{-1}(1 - a) \in P \quad \Rightarrow a - 1 \in P \quad \Rightarrow 1 < a.$$

24. $$\left.\begin{array}{llll} -1 < a & \Rightarrow a + 1 \in P & & \\ a < 0 & \Rightarrow 0 - a = -a \in P & \Rightarrow (-a)^{-1} \in P & \overset{?}{\Rightarrow} -(a^{-1}) \in P \end{array}\right\} \Rightarrow$$
$$\Rightarrow -(a^{-1})(a + 1) \in P \quad \Rightarrow -a^{-1}a - a^{-1} = -1 - a^{-1} \in P \quad \Rightarrow a^{-1} < -1 \quad \Rightarrow 1/a < -1$$

25. First, show that P' defines positive numbers as per Definition 1:

- (closure) $\forall a', b' \in R' : \exists a, b \in R : \phi a = a', \phi b = b'$. Because P is positive, $a + b, ab \in P$ so $\phi(a + b), \phi(ab) \in P'$.

  Because ϕ is a ring isomorphism, $\phi(a + b) = \phi a + \phi b = a' + b' \in P'$ and $\phi(ab) = \phi a \cdot \phi b = a' \cdot b' \in P'$.

- (trichotomy) $\forall a' \in R' : \exists a \in R : \phi a = a'$. Because P is positive:

$$\vee \begin{cases} a \in P & \Rightarrow a' = \phi a \in P' \\ -a \in P & \Rightarrow -a' = -\phi a \overset{?}{=} \phi(-a) \in P' \\ a = 0 & \Rightarrow a' = \phi a = 0' \end{cases}$$

Then, show that the ordering induced by P' is the same as <:
$\forall a', b' \in R' : \exists a, b \in R : \phi a = a', \phi b = b'$:

$$a < b \quad \Leftrightarrow \quad b - a \in P \quad \Leftrightarrow \quad \phi(b - a) \in P' \quad \Leftrightarrow \quad \phi(b - a) = \phi b - \phi a = b' - a' \in P' \quad \Leftrightarrow \quad a' < b'.$$

26.
- (closure) $\forall a, b \in S : a, b \in P$:

$$a + b \overset{\text{ring}}{\in} S \quad \wedge \quad a + b \quad \overset{\text{Definition 1}}{\in} \quad P \quad \Rightarrow a + b \in P \cap S$$
$$a \cdot b \overset{\text{ring}}{\in} S \quad \wedge \quad a \cdot b \quad \overset{\text{Definition 1}}{\in} \quad P \quad \Rightarrow a \cdot b \in P \cap S$$

- (trichotomy) $\forall a \in S$:

$$a \in R \quad \Rightarrow \begin{cases} a \in P & \Rightarrow a \in P \cap S \\ -a \in P & \Rightarrow -a \overset{\text{group}}{\in} S \quad \Rightarrow -a \in P \cap S \\ a = 0 & \end{cases}$$

27. Let P be such that $p \in P$ if and only if $0 < p$. Show that P is a well-defined set of positive numbers:

- (closure) $\forall a, b \in P$:

$$0 < a, b \quad \overset{\text{isotonicity}}{\Rightarrow} \quad b < a + b \quad \Rightarrow 0 < b < a + b \quad \overset{\text{transitivity}}{\Rightarrow} \quad 0 < a + b \quad \Rightarrow a + b \in P$$
$$0 < a, b \quad \overset{\text{isotonicity}}{\Rightarrow} \quad a \cdot 0 < a \cdot b \quad \Rightarrow a < ab \quad \Rightarrow 0 < a < ab \quad \overset{\text{transitivity}}{\Rightarrow} \quad 0 < ab \quad \Rightarrow ab \in P$$

- (trichotomy) $\forall a \in P$:

$$\vee\begin{cases} a < 0 \\ a = 0 \\ 0 < a \end{cases} \Rightarrow \vee\begin{cases} 0 - a \in P \\ a = 0 \\ a = 0 \in P \end{cases} \Rightarrow \vee\begin{cases} -a \in P \\ a = 0 \\ a \in P \end{cases}$$

Now $\forall a, b \in R$: $a < b \quad \Leftrightarrow \quad 0 < b - a \quad \Leftrightarrow \quad b - a \in P \quad \Leftrightarrow \quad a <_P b$, so P implies the same relation.

28. For all a, b:

$$\vee\begin{cases} a = b \\ a = -b \end{cases} \Rightarrow \vee\begin{cases} a - b = 0 \\ a + b = 0 \end{cases} \Rightarrow (a+b)(a-b) = a^2 - b^2 = 0 \quad \Rightarrow a^2 = b^2$$

$$\wedge\begin{cases} a \neq b \\ a \neq -b \end{cases} \Rightarrow \wedge\begin{cases} a - b \neq 0 \\ a + b \neq 0 \end{cases} \Rightarrow (a+b)(a-b) = a^2 - b^2 \neq 0 \quad \Rightarrow a^2 \neq b^2$$

so $a^2 = b^2 \quad \Leftrightarrow \quad a = \pm b$. So $a^{2n+1} = b^{2n+1} \quad \Rightarrow \left(a^2\right)^n a = \left(b^2\right)^n b \quad \Rightarrow a = b$.

29. Ordering the following elements of $R[x, y]$: $\begin{matrix} x^{-1}y^{-1} & y^{-1} & xy^{-1} \\ x^{-1} & 1 & x \\ x^{-1}y & y & xy \end{matrix}$:

$R[x][y]$

low	low	$xy < x < xy^{-1} < y < 1 < y^{-1} < x^{-1}y < x^{-1} < x^{-1}y^{-1}$
low	high	$xy^{-1} < x < xy < y^{-1} < 1 < y < x^{-1}y^{-1} < x^{-1} < x^{-1}y$
high	low	$x^{-1}y < x^{-1} < x^{-1}y^{-1} < y < 1 < y^{-1} < xy < x < xy^{-1}$
high	high	$x^{-1}y^{-1} < x^{-1} < x^{-1}y < y^{-1} < 1 < y < xy^{-1} < x < xy$

$R[y][x]$

low	low	$xy < y < x^{-1}y < x < 1 < x^{-1} < xy^{-1} < y^{-1} < x^{-1}y^{-1}$
low	high	$x^{-1}y < y < xy < x^{-1} < 1 < x < x^{-1}y^{-1} < y^{-1} < xy^{-1}$
high	low	$xy^{-1} < y^{-1} < x^{-1}y^{-1} < x < 1 < x^{-1} < xy < y < x^{-1}y$
high	high	$x^{-1}y^{-1} < y^{-1} < xy^{-1} < x^{-1} < 1 < x < x^{-1}y < y < xy$

§6.1 Homomorphisms and Factor Rings

♥ The concepts of *normal* and *ideal* didn't accidentally result in factor groups and rings— their requirements were defined precisely so that the resulting groups and rings would be well-defined:
N a normal group: $\forall g \in G$: $\quad g + N = N + g$ (Definition 3.1.19)
N an ideal ring: $\forall r \in R$: $\quad r + N \subseteq N, \quad N + r \subseteq N$ (Definition 6.1.10)

1. A ring endomorphism ϕ of $\mathbb{Z}$ by Theorem 3 has to have $\phi 0 = 0$, and $\phi 1 = 1$ iff ϕR has unity $1 \neq 1$ or else $\phi 1 = 0$. So $\phi(0,0) = (0,0)$ and:

$$\begin{array}{ll}
\phi(1,0)=(1,0) & \phi(0,1)=(0,1) \\
\phi(1,0)=(1,0) & \phi(0,1)=(0,0) \\
\phi(1,0)=(0,1) & \phi(0,1)=(1,0) \\
\phi(1,0)=(0,1) & \phi(0,1)=(0,0) \\
\phi(1,0)=(1,1) & \phi(0,1)=(0,0) \\
\phi(1,0)=(0,0) & \phi(0,1)=(0,1) \\
\phi(1,0)=(0,0) & \phi(0,1)=(1,0) \\
\phi(1,0)=(0,0) & \phi(0,1)=(1,1) \\
\phi(1,0)=(0,0) & \phi(0,1)=(0,0)
\end{array}$$

completely define the only possibilities.

2. For all even n there is a $\mathbb{Z}_n/\mathbb{Z}_m \cong \mathbb{Z}_{n/m} = \mathbb{Z}_2$, whereas for all odd n there is no element i such that $i^2 = 0$ and so will never have a coset such that $(i+H)^2 = H$ or a subring isomorphic to $\mathbb{Z}_2$.

3. The ideals and their isomorphic subrings are:

$$\begin{array}{ll}
12\mathbb{Z}_1 \subset \mathbb{Z}_{12} & \mathbb{Z}_{12}/12\mathbb{Z}_1 \cong \mathbb{Z}_{12} \\
6\mathbb{Z}_2 \subset \mathbb{Z}_{12} & \mathbb{Z}_{12}/6\mathbb{Z}_2 \cong \mathbb{Z}_6 \\
4\mathbb{Z}_3 \subset \mathbb{Z}_{12} & \mathbb{Z}_{12}/4\mathbb{Z}_3 \cong \mathbb{Z}_4 \\
3\mathbb{Z}_4 \subset \mathbb{Z}_{12} & \mathbb{Z}_{12}/3\mathbb{Z}_4 \cong \mathbb{Z}_3 \\
2\mathbb{Z}_6 \subset \mathbb{Z}_{12} & \mathbb{Z}_{12}/2\mathbb{Z}_6 \cong \mathbb{Z}_2 \\
1\mathbb{Z}_{12} \subseteq \mathbb{Z}_{12} & \mathbb{Z}_{12}/1\mathbb{Z}_{12} \cong \mathbb{Z}_1
\end{array}$$

4. $2\mathbb{Z} = \{\ldots,-4,-2,0,2,4,\ldots\}$, $8\mathbb{Z} = \{\ldots,-16,-8,0,8,16,\ldots\}$; $2\mathbb{Z}/8\mathbb{Z} = \{0+8\mathbb{Z}, 2+8\mathbb{Z}, 4+8\mathbb{Z}, 6+8\mathbb{Z}\}$

$+$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$2+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$	$0+8\mathbb{Z}$
$4+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$
$6+8\mathbb{Z}$	$6+8\mathbb{Z}$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$

$\cdot$	$0+8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$
$2+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$
$4+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$	$0+8\mathbb{Z}$
$6+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$	$0+8\mathbb{Z}$	$4+8\mathbb{Z}$

$2\mathbb{Z}/8\mathbb{Z} \not\cong \mathbb{Z}_4$ because while $\mathbb{Z}_4$ has a multiplicative identity, $2\mathbb{Z}/8\mathbb{Z}$ does not.

5. Insert "is a *ring* homomorphism".

6. Change "additive subgroup" to 'subring'.

7. Change to $\{r \in R \mid \phi r = 0'\}$.

8. $\forall f,g \in F$: $\delta(f+g) = f' + g' = \delta f + \delta g$; $\delta(f \cdot g) = f \cdot g' + g' \cdot f = f\delta g + g\delta f$, so δ is a group but not a ring isomorphism. The subring C of Example 12 is the kernel of δ. If δ would have been an homomorphism, then C would have been an ideal in F.

9. Let $\phi : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z} : n \mapsto (n,0)$, then $\phi 1 = (1,0) \notin (1,1) = 1_{\mathbb{Z}\times\mathbb{Z}}$ but $\forall (m,0) \in \phi\mathbb{Z}$: $(m,0)\cdot(1,0) = (m,0)$ so $(1,0)$ is the multiplicative identity of $\phi\mathbb{Z}$.

10. a. true (Theorem 17)
    b. false (cf. last paragraph of the section)
    c. true (Corollary 6)
    d. false ($\forall q \in \mathbb{Q}$: $q \cdot \sqrt{2} \notin \mathbb{Q}$)
    e. true (Definition 10)
    f. false (Example 12)
    g. true (because multiplication is defined by means of multiplication of representatives, which is commutative)

h. true (Example 8)

i. true (Obviously, if $N=R$ then $1\in N$. Conversely, if $1\in N$ then $\forall r\in R: r=r\cdot 1\in N \quad \Rightarrow R=N$)

j. true

11. No. (See discussion after Example 2.4)
12. See Example 2.1.
13. See Example 2.4.
14. See Example 2.2.
15. $\left\langle\left(1,1\right)\right\rangle\subset\mathbb{Z}\times\mathbb{Z}$, but from $\left(1,0\right)\cdot\left(1,1\right)=\left(1,0\right)\notin\left\langle\left(1,1\right)\right\rangle$ is not ideal.
16. a. Because the expression "$rs=sr$" is a statement about the ring R and not about the quotient ring.

b. "Then $\left(r+N\right)\left(s+N\right)=\left(s+N\right)\left(r+N\right)$ for all $r,s\in R$"

c. Suppose R/N is commutative. $\forall r,s\in R$:

$$\left(r+N\right)\left(s+N\right)=\left(s+N\right)\left(r+N\right) \quad \Rightarrow \left(r+N\right)\left(s+N\right)-\left(s+N\right)\left(r+N\right)=0_{R/N}=N,$$

so $\forall n_r,n_s,n_r',n_s'\in N$: $\exists n\in N$:

$$\left(r+n_r\right)\left(s+n_s\right)-\left(s+n_s'\right)\left(r+n_r'\right)=\left(rs+rn_s+n_rs+n_rn_s\right)-\left(sr+sn_r'+n_s'r+n_s'n_r'\right)=n$$

$$\Rightarrow rs-sr=n-\left(rn_s+n_rs+n_rn_s\right)+\left(sn_r'+n_s'r+n_s'n_r'\right)\in N$$

because N is ideal. Conversely, suppose that $\forall r,s\in R$: $\quad rs-sr\in N$. Then $\forall n_r,n_s,n_r',n_s'\in N$:

$$\left(r+n_r\right)\left(s+n_s\right)-\left(s+n_s'\right)\left(r+n_r'\right)=\ldots=\left(rs-sr\right)+\left(rn_s+n_rs+n_rn_s\right)-\left(sn_r'+n_s'r+n_s'n_r'\right)\in N$$

so

$$\left(r+N\right)\left(s+N\right)-\left(s+N\right)\left(r+N\right)=N=0_{R/N} \quad \Rightarrow \left(r+N\right)\left(s+N\right)=\left(s+N\right)\left(r+N\right)$$

and R/N is commutative.

17. First, show that $R=\left\{_{a,a'\in\mathbb{Z}} \quad a+a'\sqrt{2}\right\}$ is well-defined as a ring. Additive closure, associativity, identity, and inverse follow fairly obviously and directly from those properties in $\mathbb{Z}$, so R is a group. Multiplicative closure and additive commutativity are similarly obvious. Additive associativity follows from $\forall a,a',b,b',c,c'\in\mathbb{Z}$:

$$\begin{aligned}\left(\left(a+a'\sqrt{2}\right)\cdot\left(b+b'\sqrt{2}\right)\right)\cdot\left(c+c'\sqrt{2}\right)&=\left(\left(ab+2a'b'\right)+\left(ab'+a'b\right)\sqrt{2}\right)\cdot\left(c+c'\sqrt{2}\right)\\&=\left(abc+2a'b'c+2ab'c'+2a'bc'\right)+\left(ab'c+a'bc+abc'+2a'b'c'\right)\sqrt{2}\\&=\left(a+a'\sqrt{2}\right)\cdot\left(\left(bc+2b'c'\right)+\left(bc'+b'c\right)\sqrt{2}\right)\\&=\left(a+a'\sqrt{2}\right)\cdot\left(\left(b+b'\sqrt{2}\right)\cdot\left(c+c'\sqrt{2}\right)\right)\end{aligned}$$

Left distributivity follows from $\forall a,a',b,b',c,c'\in\mathbb{Z}$:

$$\begin{aligned}\left(a+a'\sqrt{2}\right)\cdot\left(\left(b+b'\sqrt{2}\right)+\left(c+c'\sqrt{2}\right)\right)&=\left(a+a'\sqrt{2}\right)\cdot\left(\left(b+c\right)+\left(b'+c'\right)\sqrt{2}\right)\\&=a\left(\left(b+c\right)+\left(b'+c'\right)\sqrt{2}\right)+a'\sqrt{2}\left(\left(b+c\right)+\left(b'+c'\right)\sqrt{2}\right)\\&=\left(a+a'\sqrt{2}\right)\left(b+b'\sqrt{2}\right)+\left(a+a'\sqrt{2}\right)\left(c+c'\sqrt{2}\right)\end{aligned}$$

Right distributivity follows similarly. Therefore R is a ring. Now, showing that $R'=\left\{_{a,a'\in\mathbb{Z}} \quad \begin{bmatrix}a & 2a'\\ a' & a\end{bmatrix}\right\}$ is a ring. Again, additive associativity, additive identity, and the additive inverse follow fairly directly from their corresponding properties in $\mathrm{M}_2\,\mathbb{Z}$ and $\mathbb{Z}$, so R' is a group. Additive closure follows from $\forall a,a',b,b'\in\mathbb{Z}$:

$$\begin{bmatrix}a & 2a'\\ a' & a\end{bmatrix}+\begin{bmatrix}b & 2b'\\ b' & b\end{bmatrix}=\begin{bmatrix}\left(a+b\right) & 2\left(a'+b'\right)\\ \left(a'+b'\right) & \left(a+b\right)\end{bmatrix}\in R'$$

and multiplicative closure $\forall a,a',b,b'\in\mathbb{Z}$:

$$\begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} \cdot \begin{bmatrix} b & 2b' \\ b' & b \end{bmatrix} = \begin{bmatrix} ab + 2a'b' & 2ab' + 2a'b \\ a'b + ab' & 2a'b' + ab \end{bmatrix} = \begin{bmatrix} \left(ab + 2a'b'\right) & 2\left(a'b + ab'\right) \\ \left(a'b + ab'\right) & \left(ab + 2a'b'\right) \end{bmatrix} \in R'.$$

Additive commutativity is again similarly obvious, and although multiplicative associativity follows directly from $\mathrm{M}_2\,\mathbb{Z}$ and $\mathbb{Z}$, it is derived in analogy to the additive property: $\forall a, a', b, b', c, c' \in \mathbb{Z}$:

$$\begin{aligned}
\begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} \cdot \left(\begin{bmatrix} b & 2b' \\ b' & b \end{bmatrix} \cdot \begin{bmatrix} c & 2c' \\ c' & c \end{bmatrix} \right) &= \begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} \cdot \begin{bmatrix} bc + 2b'c' & 2bc' + 2b'c \\ b'c + bc' & 2b'c' + bc \end{bmatrix} \\
&= \begin{bmatrix} a\left(bc + 2b'c'\right) + 2a'\left(b'c + bc'\right) & a\left(2bc' + 2b'c\right) + 2a'\left(2b'c' + bc\right) \\ a'\left(bc + 2b'c'\right) + a\left(b'c + bc'\right) & a'\left(2bc' + 2b'c\right) + a\left(2b'c' + bc\right) \end{bmatrix} \\
&= \begin{bmatrix} abc + 2ab'c' + 2a'b'c + 2a'bc' & 2abc' + 2ab'c + 4a'b'c' + 2a'bc \\ a'bc + 2a'b'c' + ab'c + abc' & 2a'bc' + 2a'b'c + 2ab'c' + abc \end{bmatrix} \\
&= \begin{bmatrix} \left(ab + 2a'b'\right)c + \left(2a'b + 2ab'\right)c' & \left(2a'b' + ab\right) \cdot 2c' + \left(2ab' + 2a'b\right)c \\ \left(a'b + ab'\right)c + \left(ab + 2a'b'\right)c' & \left(ab' + a'b\right) \cdot 2c' + \left(2a'b' + ab\right)c \end{bmatrix} \\
&= \begin{bmatrix} ab + 2a'b' & 2ab' + 2a'b \\ a'b + ab' & 2a'b' + ab \end{bmatrix} \cdot \begin{bmatrix} c & 2c' \\ c' & c \end{bmatrix} \\
&= \left(\begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} \cdot \begin{bmatrix} b & 2b' \\ b' & b \end{bmatrix} \right) \cdot \begin{bmatrix} c & 2c' \\ c' & c \end{bmatrix}
\end{aligned}$$

Distributivity follows directly from $\mathrm{M}_2\,\mathbb{Z}$, so R' is a ring. Let $\phi : R \to R' : a + a'\sqrt{2} \mapsto \begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix}$. Then:

- (additive homomorphy) $\forall a, a', b, b' \in \mathbb{Z}$:

$$\begin{aligned}
\phi\left(\left(a + a'\sqrt{2} \right) + \left(b + b'\sqrt{2} \right) \right) &= \phi\left(\left(a + b\right) + \left(a' + b'\right)\sqrt{2} \right) \\
&= \begin{bmatrix} \left(a + b\right) & 2\left(a' + b'\right) \\ \left(a' + b'\right) & \left(a + b\right) \end{bmatrix} = \begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} + \begin{bmatrix} b & 2b' \\ b' & b \end{bmatrix} \\
&= \phi\left(a + a'\sqrt{2} \right) + \phi\left(b + b'\sqrt{2} \right)
\end{aligned}$$

- (multiplicative homomorphy) $\forall a, a', b, b' \in \mathbb{Z}$:

$$\begin{aligned}
\phi\left(\left(a + a'\sqrt{2} \right) \cdot \left(b + b'\sqrt{2} \right) \right) &= \phi\left(\left(ab + 2a'b'\right) + \left(ab' + a'b\right)\sqrt{2} \right) \\
&= \begin{bmatrix} \left(ab + 2a'b'\right) & 2\left(ab' + a'b\right) \\ \left(ab' + a'b\right) & \left(ab + 2a'b'\right) \end{bmatrix} = \begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} \cdot \begin{bmatrix} b & 2b' \\ b' & b \end{bmatrix} \\
&= \phi\left(a + a'\sqrt{2} \right) \cdot \phi\left(b + b'\sqrt{2} \right)
\end{aligned}$$

- (isomorphy) $\forall a, a' \in \mathbb{Z}$: $\phi\left(a + a'\sqrt{2} \right) = 0_{R'} \quad \Rightarrow \begin{bmatrix} a & 2a' \\ a' & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \Rightarrow a, a' = 0 \quad \Rightarrow \operatorname{Ker} \phi = 0_R$

so ϕ is a ring isomorphism, and $R \cong R'$.

18. Following Theorem 2.5, if $N \subseteq R$ is ideal and contains any nonzero element of R, it contains a unit and therefore unity, and then $N = R$. So a field contains no proper nontrivial ideals, and by the Fundamental Homomorphism Theorem any field homomorphism is either trivial or identity.

19. Exercise 3.1.49 already shows that $\psi\phi$ is a group homomorphism. $\forall g, h \in R$:

$$\psi\phi\left(gh\right) = \psi\left(\phi\left(gh\right)\right) \overset{\phi \text{ homomorphism}}{=} \psi\left(\phi g \cdot \phi h\right) \overset{\psi \text{ homomorphism}}{=} \psi\phi g \cdot \psi\phi h.$$

20. $\forall a, b \in R$:

$$\phi(a+b) = (a+b)^p = +_{0\le i\le p}\binom{p}{i}a^{p-i}b^i = +_{0\le i\le p}\frac{p!}{(p-i)!\,i!}a^{p-i}b^i$$
$$= \frac{p!}{p!\,0!}a^p b^0 + \left(+_{0<i<p}\; p\cdot\frac{(p-1)!}{(p-i)!\,i!}a^{p-i}b^i\right) + \frac{p!}{0!\,p!}a^0 b^p$$
$$= a^p + \left(+_{0<i<p}\; 0\right) + b^p = a^p + b^p$$

The middle terms vanish because p is the characteristic of the ring.

$\phi(ab) = (ab)^p \overset{\text{commutative}}{=} a^p b^p = \phi a \cdot \phi b$.

¿Why does it matter that p is prime?

21. Suppose that $\phi 1 \ne 1'$. Then $\forall r \in \phi R^*$: $(\phi 1 - 1')r = \phi 1 \cdot r - 1' \cdot r = r - r = 0$, where $r, \phi 1 - 1' \ne 0'$ so that R' has divisors of zero. Consequently, if R' has no divisors of zero, then $\phi 1 = 1'$. (Due to Doug Rosenberg)

22. a. $\forall a' \in \phi R, n' \in \phi N$: $\exists a \in R, n \in N : \phi a = a', \phi n = n'$:

$an \in N \quad \Rightarrow \phi(an) \in \phi N \quad \Rightarrow \phi a \cdot \phi n \in \phi N \quad \Rightarrow a' \cdot n' \in \phi N \quad \Rightarrow a' \cdot \phi N \subseteq \phi N$.

Similarly, $\phi N \cdot a' \subseteq \phi N$, so $\phi N \lhd \phi R$.

b. $2\mathbb{Z} \lhd \mathbb{Z}$. Let $\phi : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z} : n \mapsto (n,n)$. Then $\phi 2\mathbb{Z} = \left\{{}_{n\in\mathbb{Z}}(n,n)\right\}$, but $(1,0)\cdot(1,1) = (1,0) \notin \phi 2\mathbb{Z}$ so $\phi 2\mathbb{Z} \ntriangleleft \mathbb{Z}\times\mathbb{Z}$.

c. If $N' \lhd R'$, then also $N' \cap \phi R \lhd \phi R$, so we only need to consider the case of $N' \lhd \phi R$. Consider the isomorphism $\mu : R/N \to \phi R$ from the Fundamental Homomorphism Theorem. By isomorphism $\mu^{\text{inv}} N' \lhd \mu^{\text{inv}} \phi R \cong R/M$, so any element $r + M \in R/M$ multiplied by $\mu^{\text{inv}} N'$ is again in $\mu^{\text{inv}} N'$. Then obviously any element $r \in R$ multiplied by $\gamma^{\text{inv}} \mu^{\text{inv}} N' = \phi^{\text{inv}} N'$ is again in $\phi^{\text{inv}} N'$, so $\phi^{\text{inv}} N' \lhd R$.

23. $\forall f \in N_S, g \in F\left[{}_i\, x_i\right]$: $\forall s \in S$: $\quad \phi_s(fg) = \phi_s f \cdot \phi_s g = 0 \cdot \phi_s g = 0 \quad \Rightarrow fg \in N_S \quad \Rightarrow N_S \lhd F\left[{}_i\, x_i\right]$.

24. By Exercise 18, any homomorphism from a field is either an isomorphism or trivial. Since every ideal subring gives rise to a homomorphism, the only ideals of a field are the field itself or the trivial field, so the only factor rings of a field are trivial or the field itself.

25. If $N \subset R$ then $R/N \supset E$ has more than one element. Since R has multiplicative identity, 1 multiplies any such element to itself, and since in the factor ring multiplication happens by representatives, 1 must be a representative of a multiplicative identity in the factor ring.

26. $\forall a \in R : I_a = \left\{{}_{x\in R}\, x \middle| ax = 0 \right\}$. So $\forall x \in I_a, r \in R$: $a \cdot rx \overset{\text{commutative}}{=} r \cdot ax = r \cdot 0 = 0 \quad \Rightarrow rx \in I_a$, and $I_a \lhd R$.

27. Any element multiplied by either ideal is again that same ideal, so the subset must multiply to itself:
$\forall r \in R, n \in N \cap N'$: $\quad n \in N \wedge n \in N' \quad \Rightarrow rn \in N \wedge rn \in N' \quad \Rightarrow rn \in N \cap N'$.

28. Lemma. A ring homomorphism/isomorphism induces a ring homomorphism/isomorphism on any of its quotient rings. Let R, R' be rings, $N \lhd R$, and $\phi : R \to R'$. By Exercise 22a, $\phi N \lhd R'$. Let γ, γ' be the canonical homomorphisms $\gamma : R \to R/N, \gamma' : R'/\phi N$. Then $\phi_* = \gamma' \phi \gamma^{\text{inv}} : R/N \to \phi R/\phi N$ is a homomorphism. Furthermore, if ϕ is an isomorphism then $\operatorname{Ker}\phi_* = \operatorname{Ker}\gamma'\phi\gamma^{\text{inv}} = \gamma\phi^{\text{inv}} \operatorname{Ker}\gamma' = \gamma\phi^{\text{inv}}\phi N = \gamma N = N = E_{R/N}$ and ϕ_* is an isomorphism.

Back to the Exercise. $\phi : R \to R'$ induces a homomorphism $\phi_* : R/N \to R'/\phi N$. Because $N' \lhd R'$, under the canonical homomorphism $\gamma : R' \to R'/\phi N$, $\gamma N' \lhd \gamma R' \Leftrightarrow \dfrac{N'}{\phi N} \lhd \dfrac{R'}{\phi N}$ so there exists a canonical homomorphism

$\beta_* : \dfrac{R'}{\phi N} \to \dfrac{R'/\phi N}{N'/\phi N} \cong \dfrac{R'}{N'}$ by the Third Isomorphism for rings (proved in Exercise 38). So

$\phi_* = \beta_* \circ \alpha_* : R/N \to R'/N'$ is a ring homomorphism.

29. Suppose there is a unit of R in the kernel of ϕ, then $0'$ would have a multiplicative inverse in R', but then the multiplicative identity in R' would be $0'$, which is counter to the definition of unity of Definition 1.16 and ϕu cannot therefore have a multiplicative inverse in R'. Conversely, suppose no unit of R is in the kernel of ϕ. Since

$u, u^{-1}, 1$ are units of R, $\phi u, \phi\left(u^{-1}\right), \phi 1 \neq 0$ and $\phi 1 = \phi\left(uu^{-1}\right) = \phi u \cdot \phi u^{-1}$, so ϕu is a unit in R'.

30. Let A be the set of all nilpotent elements of R. First, A is a subring because 0 is obviously nilpotent and $\forall a, b \in A : \exists n, m \in \mathbb{Z}^+ : a^n = 0, b^m = 0$:

- (additive closure) Consider $\left(a+b\right)^{n+m} = +_{0 \leq i \leq n+m} \begin{pmatrix} n+m \\ i \end{pmatrix} a^{\left(n+m\right)-i} b^i$. Since the sum of the powers of a and b in each of the terms is always $n+m$, either the power of a is at least n or that of b is at least m, so that the terms all vanish and $a+b$ is nilpotent.
- (multiplicative closure) $\left(ab\right)^{n+m} \overset{\text{commutative}}{=} a^{n+m} b^{n+m} = a^n a^m b^n b^m = 0a^m + b^n 0 = 0$, so ab is nilpotent.

Then $\forall a \in A, \forall r \in R : \exists n \in \mathbb{Z}^+ : a^n = 0$, so $\left(ar\right)^n \overset{\text{commutative}}{=} a^n r^n = 0r^n = 0$ and ar is nilpotent. So A is ideal.

31. The elements in the nilradical of $\mathbb{Z}_n$ are those that contain all the prime factors of n:
$\mathbb{Z}_{12} : 12 = 2^2 3$ has $\left\{0, 6\right\}$
$\mathbb{Z}_{32} : 32 = 2^5$ has $\left\{0, 2, 4, \ldots, 30\right\}$
$\mathbb{Z} \cong$ "$\mathbb{Z}_\infty$" has $\left\{0\right\}$

32. Obviously, $0 + N$ is nilpotent in R/N. Since multiplication in the factor ring occurs by representatives in N, and no elements in $R \setminus N$ are nilpotent, it is also the only nilpotent element of R/N.

33. Let $r \in R$. Since the nilradical of R/N is itself, there is an r_N such that $r \in r_N + N$ and r_N nilpotent, and there is an $n \in N$ such that $r = r_N + n$ and n nilpotent. By the proof of additive closure of nilpotents in a commutative ring in Exercise 30, r is also nilpotent. Therefore R is its own nilradical.

34. First, show that the radical in fact forms a subring. $\forall a, b \in \sqrt{N} : \exists n, m \in \mathbb{Z}^+ : a^n, b^m \in \sqrt{N}$:

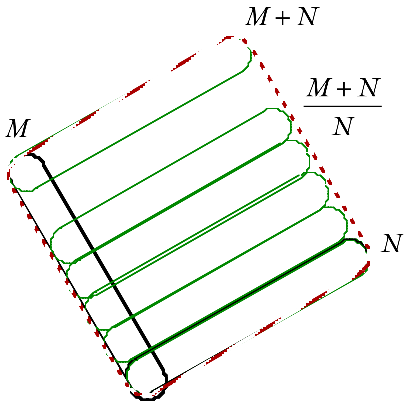
- (identity) Since N is an ideal and a subring, $0 \in N$ and because $0' = 0$, $0 \in \sqrt{N}$.
- (additive closure) Consider $\left(a+b\right)^{n+m} = +_{0 \leq i \leq n+m} \begin{pmatrix} n+m \\ i \end{pmatrix} a^{\left(n+m\right)-i} b^i$. Since the sum of the powers of a and b in each of the terms is always $n+m$, either the power of a is at least n or that of b is at least m, so each of the terms is of the form $a^j a^n b^k b^m = a^j n_a b^k n_b \overset{\text{commutative}}{=} a^j b^k n_a n_b = a^j b^k n_{ab}$, where $n_a, n_b, n_{ab} \in N$. Because n_{ab} is an element of the ideal, $a^j b^k n_{ab} \in N$ so each of the terms is as well. Because the ideal is a subring and closed under addition, the entire sum is in the ideal.
- (multiplicative closure) $\left(ab\right)^{n+m} = a^{n+m} b^{n+m} = a^n a^m + b^n b^m = n_a a^m + b^n n_b$, where $n_a, n_b \in N$. Similarly, $n_a a^m, b^m n_b$ and the sum is in the ideal.

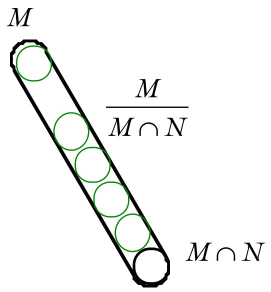
So $\sqrt{N}$ is a subring. $\forall n \in \sqrt{N} : \exists i \in \mathbb{Z}^+ : n^i = n_n \in N$. Then $\forall r \in R$: $\left(rn\right)^i \overset{\text{commutative}}{=} r^i n^i = r^i n_n \in N$, so $\sqrt{N} \lhd N$.

35. a. $\mathbb{R} \lhd \mathbb{C}$; $i \in \sqrt{\mathbb{R}}, i \notin \mathbb{R}$.
b. $2\mathbb{Z} \lhd \mathbb{Z}$, $\sqrt{2\mathbb{Z}} = 2\mathbb{Z}$.

36. The radical of N is the set of all the elements that by some power end up in N. The nilradical of R/N is the cosets of N that by some power equal the coset $0 + N$. So $\sqrt{N}$ is precisely the elements of R that are representatives of an element of the nilradical of R/N.

37.





First, show that $M+N$ is a ring. $\forall m+n, m'+n' \in M+N$:

- (identity) $0 = 0+0 \in M+N$;
- (additive closure) $(m+n)+(m'+n') = (m+m')+(n+n') \in M+N$;
- (multiplicative closure) $(m+n)\cdot(m'+n') = mm'+mn'+nm'+nn' = m_m+m_n+n_m+n_n = m_{mn}+n_{mn} \in M+N$,

where $m_m, m_n, m_{mn} \in M$, $n_m, n_n, n_{mn} \in N$.

Then show that $M+N \triangleleft R$: $\forall m+n \in M+N, \forall r \in R$: $r(m+n) = rm+rn = m_r+n_r \in M+N$, where $m_r \in M, n_r \in N$.

Now, follow the proof of Theorem 4.1.5. Let $\gamma : R \to R/N$ be the canonical homomorphism. Under γ, then, $M \subseteq R \quad \Rightarrow \gamma M \subseteq R/N$. First, consider the restriction $\gamma\big|_H : M \to \gamma M$ which is a homomorphism with $\mathrm{Ker}\gamma\big|_H = N\cap M$. By the Fundamental Homomorphism Theorem there exists an isomorphism $\mu_1 : \frac{M}{N\cap M} \to \gamma M$. Second, consider the restriction $\gamma\big|_{M+N} : M+N \to \gamma(M+N)$. Now $\forall n \in N : \gamma n = N = 1_{R/N}$, so $\gamma(M+N) = \gamma M$ and $\gamma\big|_{M+N} : M+N \to \gamma M$ with $\mathrm{Ker}\gamma\big|_{M+N} = N$ and there similarly exists an isomorphism $\mu_2 : \frac{M+N}{N} \to \gamma M$. Therefore, $\frac{M}{N\cap M} \cong \frac{M+N}{N}$.

38. Follow the proof of Theorem 4.1.7. Let $\phi : R \to \frac{R/M}{N/M} : r \mapsto (r+M)+N/M$. First, show that ϕ is a ring homomorphism. $\forall a,b \in R$:

- (addition) $\phi(a+b) = ((a+b)+M)+\frac{N}{M} \overset{(*)}{=} ((a+M)+(b+M))+\frac{N}{M} \overset{(*)}{=} \left((a+M)+\frac{N}{M}\right)+\left((b+M)+\frac{N}{M}\right) = \phi a+\phi b$, where "(*)" holds because coset addition in a ring is well-defined.
- (multiplication) $\phi(ab) = (ab+M)+\frac{N}{M} = ((a+M)\cdot(b+M))+\frac{N}{M} = \left((a+M)+\frac{N}{M}\right)\cdot\left((b+M)+\frac{N}{M}\right) = \phi a\cdot\phi b$, where "(*)" holds because coset multiplication in a ring is well-defined.

The identity element in $\frac{R/M}{N/M}$ is $(0+M)+\frac{N}{M}$ and $\mathrm{Ker}\,\phi = N$, so by the Fundamental Homomorphism Theorem $\frac{R}{N} \cong \frac{R/M}{N/M}$.

39. Show that $\phi : \mathbb{C} \to \mathrm{M}_2\,\mathbb{R} : a+a'i \mapsto \begin{bmatrix} a & a' \\ -a' & a \end{bmatrix}$ is an isomorphism. $\forall a+a'i, b+b'i \in \mathbb{C}$:

- (addition)

$$\phi\Big(\big(a+a'i\big)+\big(b+b'i\big)\Big)=\phi\Big(\big(a+b\big)+\big(a'+b'\big)i\Big)=\begin{bmatrix}a+b & a'+b'\\ -a'-b' & a+b\end{bmatrix}=\begin{bmatrix}a & a'\\ -a' & a\end{bmatrix}+\begin{bmatrix}b & b'\\ -b' & b\end{bmatrix}=\phi\big(a+a'i\big)+\phi\big(b+b'i\big)$$

- (multiplication)

$$\phi\Big(\big(a+a'i\big)\cdot\big(b+b'i\big)\Big)=\phi\Big(\big(ab-a'b'\big)+\big(ab'+a'b\big)i\Big)$$

$$=\begin{bmatrix}ab-a'b' & ab'+a'b\\ -ab'-a'b & ab-a'b'\end{bmatrix}=\begin{bmatrix}a & a'\\ -a' & a\end{bmatrix}\cdot\begin{bmatrix}b & b'\\ -b' & b\end{bmatrix}=\phi\big(a+a'i\big)\cdot\phi\big(b+b'i\big)$$

40. a. $\forall x,y\in\langle R,+\rangle$: $\gamma_a\big(x+y\big)=a\cdot\big(x+y\big)\overset{\text{ring}}{=}ax+ay=\gamma_a x+\gamma_b x$.

b. Show that it is a ring: $\forall\gamma_a,\gamma_b\in R'$:

- (identity) $\gamma_1:R\to R':x\mapsto 1\cdot x=x$ is the identity of $\text{End}\langle R,+\rangle$;
- (additive closure): $\forall x\in R$: $\big(\gamma_a+\gamma_b\big)x=\gamma_a x+\gamma_b x=a\cdot x+b\cdot x=\big(a+b\big)\cdot x=\gamma_{a+b}x$, so $\gamma_a+\gamma_b=\gamma_{a+b}\in R'$;
- (multiplicative closure) $\forall x\in R$: $\big(\gamma_a\cdot\gamma_b\big)x=\gamma_a\big(\gamma_b x\big)=\gamma_a\big(b\cdot x\big)=a\cdot\big(b\cdot x\big)=\big(a\cdot b\big)x=\gamma_{a\cdot b}x$ so $\gamma_a\cdot\gamma_b=\gamma_{a\cdot b}\in R'$.

c. Let $\phi:R\to R':a\mapsto\gamma_a$. $\forall a,b\in R$:

- (addition) $\phi\big(a+b\big)=\lambda_{a+b}\overset{\text{(b.)}}{=}\lambda_a+\lambda_b=\phi a+\phi b$;
- (multiplication) $\phi\big(a\cdot b\big)=\lambda_{a\cdot b}\overset{\text{(b.)}}{=}\lambda_a\cdot\lambda_b=\phi a\cdot\phi b$;
- (isomorphy) The identity of R' is λ_1, so $\text{Ker}\,\phi=\{1\}$.

So $R\cong R'$. λ_a is a permutation, and every ring R is thus isomorphic to a ring of permutations.

§6.2 Prime and Maximal Ideals

♥ 9 As a proof of concept, restate Theorem 9 in a format that shows the hierarchial top-down structure of the proof. This is truer to the $1\frac{1}{2}$-dimensional nature of a proof than the flattened linear text, and more consistent than the alternating bidirectional 'imply/infer' logic of the text stream. Because it obviates mentally reconstructing the true structure of the proof and permits the reader to selectively ignore details of the proof, it should theoretically be easier to understand.

M is a maximal ideal of $R\Leftrightarrow R/M$ is a field
(R/M is a field $\Leftarrow M$ is a maximal ideal) ($\Leftarrow$
R/M is a commutative ring with unity ($\Leftarrow$
R is a commutative ring with unity
)
R/M has multiplicative inverses ($\Leftarrow$
Let $\forall a\in R:N_a=\{_{r\in R,m\in M}\ ra+m\}$.
N_a is a group under addition ($\Leftarrow$
N_a is closed ($\Leftarrow$
$\forall ra+m,r'a+m'\in N_a$: $\big(ra+m\big)+\big(r'a+m'\big)=\big(r+r'\big)a+\big(m+m'\big)\in N_a$
) $\wedge$
N_a has identity ($\Leftarrow$
$\forall ra+m:\big(0a+0\big)+\big(ra+m\big)=\big(0+r\big)a+\big(0+m\big)=ra+m$
) $\wedge$
N_a has inverses ($\Leftarrow$
$\forall ra+m\in N_a$: $\Big(\big(-r\big)a+\big(-m\big)\Big)+\big(ra+m\big)=\big(-r+r\big)a+\big(-m+m\big)=0a+0=0_{N_a}$
)
),

```
        $N_a \lhd R$ ( $\Leftarrow$
            $\forall ra + m \in N_a$:
            $\forall g \in R: g\left(ra + m\right) = \left(gr\right)a + gm \in N_a$ ( $\Leftarrow$
                $gr \in R$,
                $gm \in R$ ( $\Leftarrow$
                    $M \lhd R$
                    )
                )
            ),
        $N_a = R$ ( $\Leftarrow$
            $N_a \supset M$ ( $\Leftarrow$
                $N_a \supseteq M$ ( $\Leftarrow$
                    $\forall m \in M : m = 0a + m \in N_a$
                    )
                $N_a \neq M$ ( $\Leftarrow$
                    $a \in N_a$ ( $\Leftarrow$
                        $a = 1a + 0 \in N_a$
                        ) $\wedge$
                    $a \notin M$ ( $\Leftarrow$
                        $a + M \neq 0_{R/M}$
                        )
                    )
                ) $\wedge$
            $M$ maximal
            ) $\Rightarrow$
        $1 \in N_a$ $\Rightarrow$
        $\exists ba + m \in N_a$ :    $ba + m = 1$ $\Rightarrow$
        $ba + M = \left(b + M\right)\left(a + M\right) = 1 + M$
        )
    ) $\wedge$
($M$ is a maximal ideal $\Leftarrow$ $R/M$ is a field) ( $\Leftarrow$
    Suppose $M$ is not maximal:  $\exists N \lhd R : R \supset N \supset M$
    $R/M$ is not a field ( $\Leftarrow$
        $R/M$ contains a proper nontrivial ideal ( $\Leftarrow$
            Let $\gamma : R \to R/M$ be the canonical homomorphism:
            $N \lhd R$ $\Rightarrow$
            $\gamma N \lhd \gamma R = R/M$ $\Rightarrow$
            $R/M \supset \gamma N \supset \left\{0 + M\right\}$
            )
        )
    )
```

We can compact the presentation with a few simple heuristics. Roughly, let ‘$\Rightarrow$’ or ‘ $\wedge$’ be implied between two lines at the same indentation level, and ‘$\Leftarrow$’ at increasing indentation:

```
$M$ is a maximal ideal of $R \Leftrightarrow$ $R/M$ is a field
 ( $R/M$ is a field $\Leftarrow$ $M$ is a maximal ideal)
    $R/M$ is a commutative ring with unity
        $R$ is a commutative ring with unity
    $R/M$ has multiplicative inverses
        Let $\forall a \in R : N_a = \left\{_{r \in R, m \in M}\ ra + m\right\}$.
        $N_a$ is a group under addition
```

closed: $\forall ra+m, r'a+m' \in N_a:\ (ra+m)+(r'a+m')=(r+r')a+(m+m')\in N_a$

identity: $\forall ra+m : (0a+0)+(ra+m)=(0+r)a+(0+m)=ra+m$

inverses: $\forall ra+m \in N_a:\ ((-r)a+(-m))+(ra+m)=(-r+r)a+(-m+m)=0a+0=0_{N_a}$

$N_a \lhd R$

$\forall ra+m \in N_a:\ \forall g \in R: g(ra+m)=(gr)a+gm \in N_a$

$gr \in R, gm \in R \Leftarrow M \lhd R$

$N_a = R$

$N_a \supset M$

$N_a \supseteq M$

$\forall m \in M : m = 0a+m \in N_a$

$N_a \neq M$

$a \in N_a \quad \Leftarrow a = 1a+0 \in N_a$

$a \notin M \quad \Leftarrow a+M \neq 0_{R/M}$

M maximal

$1 \in N_a \quad \Rightarrow \exists ba+m \in N_a:\quad ba+m=1$

$ba+M=(b+M)(a+M)=1+M$

(M is a maximal ideal $\Leftarrow$ R/M is a field)

Suppose M is not maximal: $\exists N \lhd R : R \supset N \supset M$

R/M is not a field

R/M contains a proper nontrivial ideal

Let $\gamma : R \to R/M$ be the canonical homomorphism:

$N \lhd R \quad \Rightarrow \gamma N \lhd \gamma R = R/M \quad \Rightarrow R/M \supset \gamma N \supset \{0+M\}$

♥ 11 R is a field $\Leftrightarrow$ R has no proper nontrivial ideals

R is a field $\Rightarrow$ R has no proper nontrivial ideals

Corollary 6

R is a field $\Leftarrow$ R has no proper nontrivial ideals

$R \cong R/E$ is a field $\quad \overset{\text{Theorem 9}}{\Leftarrow} \quad E \lhd R$ maximal $\Leftarrow$ R has no proper nontrivial ideals

♥ 15 N is prime $\Leftrightarrow$ $(ab \in N \quad \Rightarrow a \in N \vee b \in N)$, so a prime ideal is such that the corresponding factor ring has no divisors of 0. In other words, $N \lhd R$ prime iff R/N is an integral domain.

♥ 16 *Maximal* and *prime* in factor rings correspond to *field* and *integral domain*.

♥ 18 Let $\phi : \mathbb{Z} \to R$ be the homomorphism from Theorem 17.

$\left(R \text{ contains a subring isomorphic to } \mathbb{Z}_n \quad \Leftarrow \operatorname{char} R > 1\right)$

$\operatorname{Ker}\phi = n\mathbb{Z}$

$\operatorname{Ker}\phi \lhd \mathbb{Z}$

$N \lhd \mathbb{Z} \quad \Rightarrow \exists s \in \mathbb{Z} : N = s\mathbb{Z}$

n is the smallest integer such that $n \cdot 1 = 0$ $\Leftarrow$ Theorem 5.2.15

$\phi\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

$\left(R \text{ contains a subring isomorphic to } \mathbb{Z} \quad \Leftarrow \operatorname{char} R = 0\right)$

$\operatorname{Ker}\phi = E$

$\forall m \in \mathbb{Z}^* : m \cdot 1 \neq 0 \quad \Leftarrow \operatorname{char} R = 0$

$\phi\mathbb{Z} \cong \mathbb{Z}/E \cong \mathbb{Z}$

♥ 24 If F is a field, then every ideal in $F[x]$ is principal

$\left(N \text{ principal} \quad \Leftarrow N \lhd F[x]\right)$

N principal $\Leftarrow N = E = \{0\} \cdot F[x]$

N principal $\Leftarrow N \supset E$

Let $g \in N$ be of minimal degree.

$(\deg g = 0 \quad \Rightarrow N = 1F[x])$

$\deg g = 0 \quad \Rightarrow g \in F \quad \overset{\text{Theorem 5}}{\Rightarrow} \quad N = F[x] = 1F[x]$

$(\deg g > 0 \quad \Rightarrow N = gF[x])$

$\forall f \in N$

$f = gq + r$ where $r = 0 \vee \deg r < \deg g \Leftarrow$ Theorem 5.6.1

$r = 0$

$r \in N$

$gq \in N$

$f \in N$

$g \in N \quad \Rightarrow gq \in N \quad \Rightarrow gq + r \in N$

$g \in N$ is of minimal degree $\deg g > 0$

$f = gq$

♥ 25 $pF[x]$ maximal $\Leftrightarrow p$ irreducible over $F[x]$

$\Rightarrow$

$\forall f, g \in F[x] : p = fg \quad \Rightarrow \deg f \geq \deg p \vee \deg g \geq \deg p$

$f \in pF[x] \vee g \in pF[x]$

$pF[x]$ prime $\quad \Leftarrow pF[x]$ maximal

$p \in pF[x]$

$\Leftarrow$

Let $N \lhd F[x]: \quad F[x] \supset N \supset pF[x]$

$\exists g \in N : N = gF[x]$

N principal $\quad \overset{\text{Theorem 24}}{\Leftarrow} \quad N \lhd F[x]$

$\exists q \in F[x] : p = gq$

$p \in N \quad \Leftarrow p \in F[x] \subset N$

$\deg g = 0 \vee \deg q = 0 \quad \Leftarrow p$ irreducible

$(\deg g = 0 \quad \Rightarrow N = F[x])$

$N = gF[x] = 1 \cdot F[x] \quad \Leftarrow g \in F$ is a unit of $F[x]$

$(\deg q = 0 \quad \Rightarrow N = pF[x])$

$g \in pF[x] \quad \Rightarrow gF[x] = pF[x]$

$g = p/q, \, q \in F$

contradiction.

♥ 27 $rs =_p 0 \quad \Rightarrow \quad r =_p 0 \vee s =_p 0$

$rs \in pF[x] \quad \Leftarrow rs =_r 0$

$pF[x]$ is prime $\quad \Leftarrow pF[x]$ is maximal

1. 1 By Example 2.7.

3 Not a division ring because it doesn't have a multiplicative inverse.

4 By Theorem 2.11.

5 Not an integral domain because it has a divisor of zero

6 By Theorem 2.9.

† and isomorphic subrings

subring	factor ring	int dom?	field?	prime?	normal?	subring
$1\mathbb{Z}_6$	$\mathbb{Z}_6/1\mathbb{Z}_6 \cong \mathbb{Z}_1$	no^3	no^6	no	no	
$2\mathbb{Z}_3$	$\mathbb{Z}_6/2\mathbb{Z}_3 \cong \mathbb{Z}_2$	yes^1	yes^4	yes	yes	$\{0,2,4\}$
$3\mathbb{Z}_2$	$\mathbb{Z}_6/3\mathbb{Z}_2 \cong \mathbb{Z}_3$	yes^1	yes^4	yes	yes	$\{0,3\}$
$6\mathbb{Z}_1$	$\mathbb{Z}_6/6\mathbb{Z}_1 \cong \mathbb{Z}_6$	no^1	no^6	no	no	

2.

subring	factor ring	int dom?	field?	prime?	normal?	subring
$1\mathbb{Z}_{12}$	$\mathbb{Z}_{12}/1\mathbb{Z}_{12} \cong \mathbb{Z}_1$	no^3	no^6	no	no	
$2\mathbb{Z}_6$	$\mathbb{Z}_{12}/2\mathbb{Z}_6 \cong \mathbb{Z}_2$	yes^1	yes^4	yes	yes	$\{0,2,4,\ldots,10\}$
$3\mathbb{Z}_4$	$\mathbb{Z}_{12}/3\mathbb{Z}_4 \cong \mathbb{Z}_3$	yes^1	yes^4	yes	yes	$\{0,3,6,9\}$
$4\mathbb{Z}_3$	$\mathbb{Z}_{12}/4\mathbb{Z}_3 \cong \mathbb{Z}_4$	no^1	no^6	no	no	
$6\mathbb{Z}_2$	$\mathbb{Z}_{12}/6\mathbb{Z}_2 \cong \mathbb{Z}_6$	no^1	no^6	no	no	
$12\mathbb{Z}_1$	$\mathbb{Z}_{12}/12\mathbb{Z}_1 \cong \mathbb{Z}_{12}$	no^1	no^6	no	no	

3.

subring	factor ring	int dom?	field?	prime?	normal?	subring
$1\mathbb{Z}_2 \times 1\mathbb{Z}_2$	$\frac{\mathbb{Z}_2 \times \mathbb{Z}_2}{1\mathbb{Z}_2 \times 1\mathbb{Z}_2} \cong \mathbb{Z}_1$	no^3	no^3	no	no	
$1\mathbb{Z}_2 \times 2\mathbb{Z}_1 \cong \mathbb{Z}_2$†	$\frac{\mathbb{Z}_2 \times \mathbb{Z}_2}{1\mathbb{Z}_2 \times 2\mathbb{Z}_1} \cong \mathbb{Z}_2$	yes^1	yes^4	yes	yes	$\{0,1\} \times \{0\}$
$2\mathbb{Z}_1 \times 2\mathbb{Z}_1 \cong \mathbb{Z}_1$	$\frac{\mathbb{Z}_2 \times \mathbb{Z}_2}{2\mathbb{Z}_1 \times 2\mathbb{Z}_1} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	no^5	no^6	no	no	

4.

subring	factor ring	int dom?	field?	prime?	normal?	subring
$1\mathbb{Z}_2 \times 1\mathbb{Z}_4$	$\mathbb{Z}_1 \times \mathbb{Z}_1 \cong \mathbb{Z}_1$	no^3	no^6	no	no	
$1\mathbb{Z}_2 \times 2\mathbb{Z}_2$	$\mathbb{Z}_1 \times \mathbb{Z}_2 \cong \mathbb{Z}_2$	yes^1	yes^4	yes	yes	$\{0,1\} \times \{0,2\}$
$1\mathbb{Z}_2 \times 4\mathbb{Z}_1$	$\mathbb{Z}_1 \times \mathbb{Z}_4 \cong \mathbb{Z}_4$	yes^1	yes^4	yes	yes	$\{0,1\} \times \{0\}$
$2\mathbb{Z}_1 \times 1\mathbb{Z}_4$	$\mathbb{Z}_2 \times \mathbb{Z}_1 \cong \mathbb{Z}_2$	yes^1	yes^4	yes	yes	$\{0\} \times \{0,1,2,3\}$
$2\mathbb{Z}_1 \times 2\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	no^5	no^6	no	no	
$2\mathbb{Z}_1 \times 4\mathbb{Z}_1$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	no^5	no^6	no	no	

5. $\mathbb{Z}_3[x]/\langle x^2+c\rangle$ is a field iff $\langle x^2+c\rangle \lhd \mathbb{Z}_3[x]$ is maximal iff x^2+c is irreducible in $\mathbb{Z}_3[x]$. If x^2+c is reducible, then it has at least one (i.c., actually two) factors of degree one $x-a$ and by the Factor Theorem then has a zero for $x=a$. By calculation, the sets A_c of zeroes a for given c are: $A_0=\{0\}$, $A_1=\varnothing$, $A_2=\{1,2\}$. So the polynomial is irreducible and the factor ring a field for $c=1$.

6. Following the procedure of Exercise 5— if x^3+x^2+c is reducible, it has to have at least one factor of degree one and a corresponding zero: $A_0=\{0,2\}$, $A_1=\{1\}$, $A_2=\varnothing$. So the factor ring is a field for $c=2$.

7. $A_0=\{2\}$, $A_1=\{1\}$, $A_2=\varnothing$; $c=2$.

8. $A_0=\{0,4\}$, $A_1=\varnothing$, $A_2=\varnothing$, $A_3=\{1,3\}$, $A_4=\{2\}$; $c=1,2$.

9. $A_0=\{2,3\}$, $A_1=\varnothing$, $A_2=\{4\}$, $A_3=\{1\}$, $A_4=\varnothing$; $c=1,4$.

10. "is a *proper* ideal"

11. The given definition is valid only if $R=\mathbb{Z}$ because prime elements have not been defined elsewhere.

12. Comparing to Definition 20, $\mathbb{Z}_p$ and $\mathbb{Q}$ can contain no nontrivial proper subfields, and any other field properly contains either of these fields— so the definition is indeed equivalent.

13. Since a principal ideal consists of all products of the field with the geneator, it is certainly the smallest ideal containing the generator. Since this defines minimal ideals for every element, all minimal ideals are principal—

therefore the definition is equivalent.

14. a. false (should find a counterexample of a factor ring that is an integral domain but not a field)
b. true (Corollary 16)
c. true (by Theorem 19 because the characteristic of $\mathbb{Q}$ is zero)
d. false (by Theorem 19 the characteristic of $\mathbb{R}$ is zero, so $\mathbb{Q}$ is the prime subfield)
e. true (Theorem 19)
f. true ($\mathbb{Q} \subset \mathbb{Q}\times\mathbb{Q}$)
g. true (Theorem 19)
h. true (if F has no divisors of zero then $F[x]$ and $F[x]/N$ don't either, so N is prime)
i. true (Theorem 24)
j. false (by Theorem 25, only if the generating polynomial is maximal)

15. $2\mathbb{Z}\times\mathbb{Z} \triangleleft \mathbb{Z}\times\mathbb{Z}$. $\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z} \cong \mathbb{Z}_2\times E \cong \mathbb{Z}_2$ is a field, so $2\mathbb{Z}\times\mathbb{Z}$ is maximal.

16. $\mathbb{Z}\times E \triangleleft \mathbb{Z}\times\mathbb{Z}$. $\mathbb{Z}\times\mathbb{Z}/\mathbb{Z}\times E \cong E\times\mathbb{Z}$ is not a field, so $\mathbb{Z}\times E \cong \mathbb{Z}$ is not maximal. Since $\mathbb{Z}$ has no divisors of zero, $\mathbb{Z}\times E$ is prime.

17. $4\mathbb{Z}\times\mathbb{Z} \triangleleft \mathbb{Z}\times\mathbb{Z}$. $\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z} \cong \mathbb{Z}_4\times E \cong \mathbb{Z}_4$ has divisors of zero, so $\mathbb{Z}_4\times E$ is not prime.

18. $\mathbb{Q}[x]/\langle x^2-5x+6\rangle$ is a field iff $\langle x^2-5x+6\rangle$ is maximal iff x^2-5x+6 is irreducible in $\mathbb{Q}[x]$. By the Factor Theorem it is irreducible iff it has no zeroes in $\mathbb{Q}$. The roots are

$$x = \frac{-(-5)\pm\sqrt{(-5)^2-4\cdot 1\cdot 6}}{2\cdot 1} = \frac{5\pm\sqrt{1}}{2} = 2,3 \in \mathbb{Q},$$

so the factor ring is not a field.

19. Following the procedure of Exercise 18:

$$x = \frac{-(-6)\pm\sqrt{(-6)^2-4\cdot 1\cdot 6}}{2\cdot 1} = \frac{6\pm\sqrt{12}}{2} = 3\pm\sqrt{3} \notin \mathbb{Q}$$

and the factor ring is therefore a field.

20. Since R is finite, so is $N\subset R$ and R/N. Since R is prime, R/N is an integral domain. By Theorem 5.2.11, R/N is a field, therefore N is maximal.

21. $\mathbb{Z}_n\times\mathbb{Z}_m$ is a ring with multiplicative identity containing $\mathbb{Z}_n\times E\cong\mathbb{Z}_n$ and $E\times\mathbb{Z}_m\cong\mathbb{Z}_m$ as subrings.

22. Idem.

23. If a ring contains subrings isomorphic to $\mathbb{Z}_p, \mathbb{Z}_q$, then it should contain a subring isomorphic to $\mathbb{Z}_{pq}$, which is not an integral domain. So any containing ring cannot be an integral domain either.

24.

25. $N \triangleleft R$ maximal $\quad\Leftrightarrow\quad R/N$ simple

$\big($suppose N not maximal $\quad\Rightarrow R/N$ not simple$\big)$

$\exists M : R \supset M \supset N, M \triangleleft R$

Let $\gamma : R \to R/N$ be the canonical homomorphism

$\gamma|_M : M \to R/N$

$M \triangleleft R \quad \Rightarrow \gamma M \triangleleft R/N$ and $\gamma M \subset R/N$

$\big($suppose R/N not simple $\quad\Rightarrow N$ not maximal$\big)$

Let γ be some canonical homomorphism.

R/N not simple $\quad\Rightarrow \exists M' \triangleleft R/N \supset M' \supset 0+N \quad\Rightarrow \gamma^{\text{inv}} M' \triangleleft R$ and $R \supset \gamma^{\text{inv}} M' \supset N$.

26.

27.

28.

29.

30. $A+B = \left\{_{a\in A, b\in B}\, a+b\right\}$.

a. Show that $A+B \subseteq R$ is a subring:

- (additive identity) $0 \in A, B \quad \Rightarrow 0 = 0+0 \in A+B$.
- (additive inverse) $\forall a+b \in A+B: -a \in A, -b \in B \quad \Rightarrow (-a)+(-b) \in A+B$:

  $(a+b)+((-a)+(-b)) = (a+(-a))+(b+(-b)) = 0+0 = 0$
- (additive closure) $\forall a, a' \in A;\ b, b' \in B$: $(a+b)+(a'+b') = (a+a')+(b+b') \in A+B$, where $a+a' \in A$, $b+b' \in B$
- (multiplicative closure) $\forall a, a' \in A;\ b, b' \in B$:

  $(a+b)\cdot(a'+b') = aa' + ab' + ba' + bb' \overset{A,B\triangleleft R}{=} a'' + a''' + b''' + b'' = a'''' + b'''' \in A+B$ where $a'' = aa' \in A, a''' = ab' \in A$ and similarly in B.

  Now show that $A+B \triangleleft R$ is an ideal: $\forall a+b \in A+B$: $\forall r \in R$: $r\cdot(a+b) = ra+rb \overset{A,B\triangleleft R}{=} a'+b'$, where $a' \in A$, $b' \in B$

  .

b. Because A, B are ideals they are subrings and contain the additive identity. Then $\forall a \in A$: $a = a+0 \in A+B \quad \Rightarrow A \subseteq A+B$ and similarly $B \subseteq A+B$.

31. $AB = \left\{_{n\in\mathbb{Z}^+} \quad +^n_{i, a_i \in A, b_i \in B}\, a_i b_i\right\}$.

a. Show that $AB \subseteq R$ is a subring.

- (additive identity) $0 = +^0_i\, a_i b_i \in AB$.
- (additive inverse) $\forall n \in \mathbb{Z}^+, a_i \in A, b_i \in B$: $\quad +^n_i\, a_i b_i \in AB$: $-a_i \in A \quad \Rightarrow +^n_i(-a_i)b_i = +^n_i - a_i b_i \in AB$:

  $\left(+^n_i\, a_i b_i\right) + \left(+^n_i - a_i b_i\right) = +^n_i\left(a_i b_i + (-a_i b_i)\right) = +^n_i 0 = 0$
- (additive closure) The sum of both sums of terms is just a larger single sum of terms.
- (multiplicative closure) $\forall n, n' \in \mathbb{Z}^+;\ a_i, a'_i \in A;\ b_i, b'_i \in B$:

  $\left(+^n_i\, a_i b_i\right)\cdot\left(+^{n'}_i\, a'_i b'_i\right) = +^n_i +^{n'}_j\, a_i b_i \cdot a'_j b'_j \overset{A,B\triangleleft R}{=} +^n_i +^{n'}_j\, a''_i \cdot b''_j = +^{n\cdot n'}_k\, a''_k b''_k \in AB$, where $a'' = a_i b_i$ and $b''_j = a'_j b'_j$.

  Then show that $AB \triangleleft R$ is ideal. $\forall n \in \mathbb{Z}^+;\ a_i \in A;\ b_i \in B$: $\forall r \in R$: $\quad r\cdot +^n_i\, a_i b_i = +^n_i\, r\cdot a_i b_i \overset{A\triangleleft R}{=} +^n_i\, a''_i b_i \in AB$, where $a''_i = r\cdot a_i$.

b. For any $+^n_i\, a_i b_i \in AB$, $+^n_i\, a_i b_i \overset{A\triangleleft R}{=} +^n_i\, a''_i \in A$ and $+^n_i\, a_i b_i \overset{B\triangleleft R}{=} +^n_i\, b''_i \in A$ where $a''_i, b''_i = a_i b_i$. So $+^n_i\, a_i b_i \in A \cap B$ and $AB \subseteq A \cap B$.

32. $A:B = \left\{_{r\in R}\ r \,\middle|\, \forall b \in B: rb \in A\right\}$.

a. First, show that $A:B \subseteq R$ is a subring.

- (additive identity) $0 \in R$: $\quad \forall b \in B$: $\quad 0\cdot b = 0 \in A \quad \Rightarrow 0 \in A:B$.
- (additive inverse) $\forall r \in A:B$, $\forall b \in B$: $\quad (-r)\cdot b = -(rb) \in A \quad \Rightarrow -r \in A:B$.
- (additive closure) $\forall r, r' \in A:B$: $\forall b \in B$: $\quad (r+r')b = rb + r'b = a + a' \in A$, where $a = rb \in A$, $a' = r'b \in A$. So $r+r' \in A:B$.
- (multiplicative closure) $\forall r, r' \in A:B$: $\forall b \in B$: $\quad (rr')b = r(r'b) = ra' \overset{A\triangleleft R}{=} a''$, where $a' = r'b \in A$ and $a'' = ra'$. So $r\cdot r' \in A:B$.

  Show that $A:B \triangleleft R$ is ideal. $\forall r \in A:B$: $\forall s \in R$: $\forall b \in B$: $\quad (rs)b \overset{\text{commutative}}{=} (rb)s = a's = a'' \in A \quad \Rightarrow rs \in A:B$, where $a' = rb \in A$ and $a'' = a's$.

33. Show that $S \subseteq \mathrm{M}_2\, F$ is a subring:

- (additive identity) $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix} \in S$.
- (additive inverse) $\forall \begin{bmatrix}a & b\\0 & 0\end{bmatrix} \in S: \quad -a, -b \in F: \quad \begin{bmatrix}-a & -b\\0 & 0\end{bmatrix} \in S: \quad \begin{bmatrix}a & b\\0 & 0\end{bmatrix} + \begin{bmatrix}-a & -b\\0 & 0\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$.
- (additive closure) follows directly from the closure of F and $\mathrm{M}_2 F$.
- (multiplicative closure) $\forall \begin{bmatrix}a & b\\0 & 0\end{bmatrix}, \begin{bmatrix}a' & b'\\0 & 0\end{bmatrix} \in S: \quad \begin{bmatrix}a & b\\0 & 0\end{bmatrix} \cdot \begin{bmatrix}a' & b'\\0 & 0\end{bmatrix} = \begin{bmatrix}aa' + b0 & ab' + b0\\0a' + 00 & 0b' + 00\end{bmatrix} = \begin{bmatrix}aa' & bb'\\0 & 0\end{bmatrix} \in S$.

Now $\forall \begin{bmatrix}a & b\\0 & 0\end{bmatrix} \in S; \quad \forall \begin{bmatrix}f_{00} & f_{01}\\f_{10} & f_{11}\end{bmatrix} \in \mathrm{M}_2 F:$
$$\begin{bmatrix}a & b\\0 & 0\end{bmatrix} \cdot \begin{bmatrix}f_{00} & f_{01}\\f_{10} & f_{11}\end{bmatrix} = \begin{bmatrix}af_{00} + bf_{10} & af_{01} + bf_{11}\\0f_{00} + 0f_{10} & 0f_{01} + 0f_{11}\end{bmatrix} = \begin{bmatrix}af_{00} + bf_{10} & af_{01} + bf_{11}\\0 & 0\end{bmatrix} \in S$$
but
$$\begin{bmatrix}f_{00} & f_{01}\\f_{10} & f_{11}\end{bmatrix} \cdot \begin{bmatrix}a & b\\0 & 0\end{bmatrix} = \begin{bmatrix}f_{00}a + f_{01}0 & f_{00}b + f_{01}0\\f_{10}a + f_{11}0 & f_{10}b + f_{11}0\end{bmatrix} = \begin{bmatrix}af_{00} & bf_{00}\\af_{10} & bf_{10}\end{bmatrix},$$
which is not necessarily in S.

34. Enumerate all the possible elements that could be contained in an ideal of $\mathrm{M}_2\,\mathbb{Z}_2$. $\left\langle \begin{bmatrix}0 & 0\\0 & 0\end{bmatrix} \right\rangle = E_{\mathrm{M}_2\,\mathbb{Z}_2}$ is the trivial ideal. Consider a matrix with one non-zero element:
$$\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} \cdot \begin{bmatrix}n_{00} & n_{01}\\n_{10} & n_{11}\end{bmatrix} = \begin{bmatrix}1n_{00} + 0n_{10} & 1n_{01} + 0n_{11}\\0n_{00} + 0n_{10} & 0n_{01} + 0n_{11}\end{bmatrix} = \begin{bmatrix}n_{00} & n_{01}\\0 & 0\end{bmatrix}$$
which we know from Exercise 33 is not an ideal. By symmetry we know that neither are any of the other principals generated by matrices with one non-zero component or with two non-zero components along a row or column. As to the other two matrices with two non-zero components, obviously $\left\langle \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \right\rangle = \left\langle \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \right\rangle = \mathrm{M}_2\,\mathbb{Z}_2$, and this implies that neither are the ideals generated by matrices with three non-zero elements proper.

§6.3 Gröbner Bases for Ideals

♥ The discussion after Example 2 states in essence that $\left\langle {}_i^n\, f_i \right\rangle = \left\{ {}_{r_i \in R} +_i r_i f_i \right\}$ are the 'principal ideals' with multiple generators, and that they are $\left\langle {}_i^r\, f_i \right\rangle = \cap_i^r \left\langle f_i \right\rangle$ the intersection of the individually-generated ideals.

♥ 4 The common zeros of $\left\{ {}_i\, f_i \right\}$ are the common zeros of $\left\langle {}_i\, f_i \right\rangle$.

♥ 5 This is just a generalization of Theorem 2.24 to multiple indeterminates: every ideal of $F[\mathbf{x}]$ is principal $\left\langle {}_i\, f_i \right\rangle$.

♥ 7 Let $f_1 : x + y - 3z - 8 = 0$ and $f_2 : 2x + y + z + 5 = 0$, then $f_3 : -y + 7z + 21 = 0$ can be formed from

$$\text{“}f = gq + r\text{”}$$

$$\downarrow$$

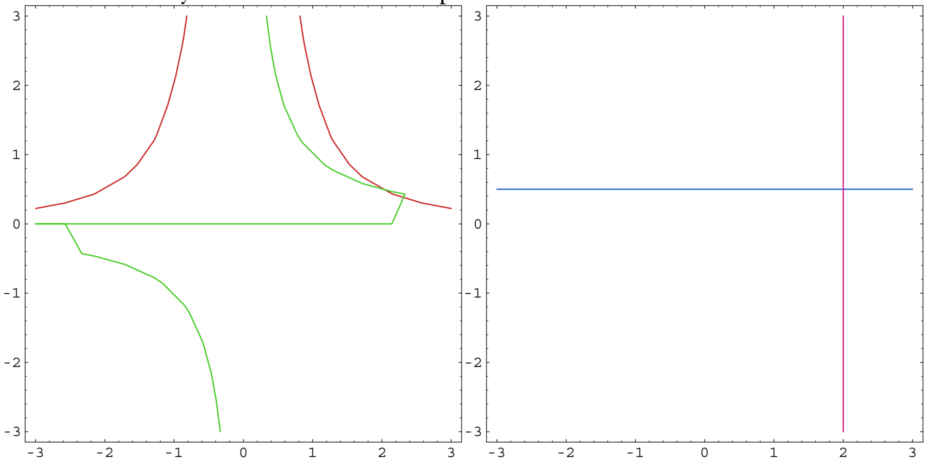
$$f_3 = f_2 - 2f_1 \quad \Leftrightarrow \quad f_2 = 2f_1 + f_3$$

$$f_3 = f_2 - 2f_1 \quad \Leftrightarrow \quad \frac{f_3}{f_1} = \frac{f_2}{f_1} - 2$$

$$\uparrow \qquad \uparrow \qquad \uparrow$$

remainder $\dfrac{\text{product}}{\text{divisor}}$ quotient

♥ 11 Keep in mind that the algebraic variety of an ideal is equal to that of any basis. In the left figure are plotted the zeros of the two original polynomials of the Example. Disregarding some plotting artifacts, it can be seen that they intersect in one point. The right figure shows the zeros of the Gröbner basis calculated in Example 13, and it can be seen that they intersect in the same point.



1. Write out the exponents of the power products, and sort them lexicographically like words:
“135, 213, 221, 300” → “300, 221, 213, 135”: $-3x^3 + 7x^2y^2z - 5x^2yz^3 + 2xy^3z^5$.

2. “025, 100, 033, 007” → “100, 033, 025, 007”: $-4x + 5y^3z^3 + 3y^2z^5 - 8z^7$.

3. “010, 100, 003, 122, 212” → “212, 122, 100, 010, 003”: $2x^2yz^2 - 2xy^2z^2 - 7x + 3y + 10z^3$.

4. “000, 101, 011, 110, 013” → “110, 101, 013, 011, 000”: $-8xy - 4xz + 3yz^3 + 2yz + 38$.

5. Write out the exponents in reverse order:
“531, 312, 122, 003” → “531, 312, 122, 003”: $2z^5y^3x - 5z^3yx^2 + 7zy^2x^2 - 3x^3$.

6. “520, 001, 330, 700” → “700, 520, 330, 001”: $-8z^7 + 3z^5y^2 + 5z^3y^3 - 4x$.

7. “010, 001, 300, 221, 212” → “300, 221, 212, 010, 001”: $10z^3 - 2z^2y^2x + 2z^2yx^2 + 3y - 7x$.

8. “000, 101, 110, 011, 310” → “310, 110, 101, 011, 000”: $3z^3y + 2zy - 4zx - 8yx + 38$.

9. $1 < z < y < x$
$< z^2 < yz < y^2 < xz < xy < x^2$
$< z^3 < yz^2 < y^2z < y^3 < xz^2 < xyz < xy^2 < x^2z < x^2y < x^3$
$< \ldots$

10. Write the sum of the exponents as an exponent and sort by degree first:
“$135^9, 213^6, 221^5, 300^3$” → “$135^9, 213^6, 221^5, 300^3$”: $2xy^3z^5 - 5x^2yz^3 + 7x^2y^2z - 3x^3$.

11. “$025^7, 100^1, 033^6, 007^7$” → “$025^7, 007^7, 033^6, 100^1$”: $3y^2z^5 - 8z^7 + 5y^3z^3 - 4x$.

12. “$010^1, 100^1, 003^3, 122^5, 212^5$” $\rightarrow$ “$212^5, 122^5, 003^3, 100^1, 010^1$”: $2x^2yz^2 - 2xy^2z^2 + 10z^3 - 7x + 3y$.

13. “$000^0, 101^2, 011^2, 110^2, 013^4$” $\rightarrow$ “$013^4, 110^2, 101^2, 011^2, 000^0$”: $3yz^3 - 8xy - 4xz + 2yz + 38$.

14.

maximum-order term

$$\begin{array}{ccc}
xy^2 - 2x & \boxed{x^2y} + 4xy & xy - y^2 \\
 & \underline{x^2y - y^2x} & \leftarrow \cdot x \\
 & 4xy + y^2x &
\end{array}$$

leaving $\left\langle xy^2 - 2x, 4xy + y^2x, xy - y^2 \right\rangle$.

15.

$$\begin{array}{ccc}
\boxed{xy} + y^3 & y^3 + z & x - y^4 \\
\underline{xy - y^5} & & \leftarrow \cdot y \\
y^5 + y^3 & &
\end{array}$$

leaving $\left\langle y^5 + y^3, y^3 + z, x - y^4 \right\rangle$.

16. Can't be reduced as required, because x^3 can't be divided by any of the $\mathrm{lp}(f_i)$.

17.

$$\begin{array}{ccc}
y^2z^3 + 3 & \boxed{y^3z^2} - 2z & y^2z^2 + 3 \\
 & \underline{y^3z^2 + 3y} & \leftarrow \cdot y \\
 & -3y - 2z &
\end{array}$$

leaving $\left\langle y^2z^3 + 3, -3y - 2z, y^2z^2 + 3 \right\rangle$.

18.

$$\begin{array}{ccc}
w + x - y + 4z - 3 & 2w + x + y - 2z + 4 & w + 3x - 3y + z - 5 \\
\cdot 2 \rightarrow & \underline{2w + 2x - 2y + 8z - 6} & \\
 & -x + 3y = 10z + 10 & \\
\cdot 1 \rightarrow & & \underline{w + x - y + 4z - 3} \\
 & & 2x - 2y - 3z - 2 \\
 & \cdot -2 \rightarrow & \underline{2x - 6y + 20z - 20} \\
 & & 4y - 23z + 18 \\
\underline{x - 3y + 10z - 10} & \leftarrow \cdot -1 & \\
w + 2y - 6z + 7 & & \\
\underline{2y - \frac{23}{2}z + 9} & & \leftarrow \cdot \frac{1}{2} \\
w + \frac{11}{2}z - 2 & & \\
 & \underline{3y - \frac{69}{4}z + \frac{27}{2}} & \leftarrow \cdot \frac{3}{4} \\
 & -x + \frac{29}{4}z - \frac{7}{2} & \\
2w + 11z - 4 & -4x + 29z - 14 &
\end{array}$$

leaving $\left\langle 2w + 11z - 4, -4x + 29z - 14, 4y - 23z + 18 \right\rangle$. Every S_{ij} has a leading term containing at least a nonzero power of w, x, or z and can thus be divided by the leading term of one of the basis polynomials. We have thus found a Gröbner basis.

19.

$$\begin{array}{cccc}
w-4x+3y-z+2 & & 2w-2x+y-2z+5 & w-10x+8y-z-1 \\
 & \cdot 2 \rightarrow & \underline{2w-8x+6y-2z+4} & \\
 & & 6x-5y+1 & \\
 & \cdot 1 \rightarrow & & \underline{w-4x+3y-z+2} \\
 & & & -6x+5y-3
\end{array}$$

leaving $\left\langle w-4x+3y-z+2, 6x-5y+1, -6x+5y-3 \right\rangle$. Since the second and third polynomials have no common zeros, the Gröbner basis is $\left\langle 1 \right\rangle$.

20.

$$\begin{array}{cc}
x^4+x^3-3x^2-4x-4 & x^3+x^2-4x-4 \\
\underline{x^4+x^3-4x^2-4x} & \leftarrow \cdot x \\
x^2-4 & \\
\cdot x \rightarrow & \underline{x^3-4x} \\
 & x^2-4
\end{array}$$

leaving $\left\langle x^2-4 \right\rangle$, which is a single-element basis and thus a Gröbner basis.

21.

$$\begin{array}{ccc}
x^4-4x^3+5x^2-2x & x^3-x^2-4x+4 & x^3-3x+2 \\
\underline{x^4-x^3-4x^2+4x} & \leftarrow \cdot x & \\
-3x^2+9x^2-6x & & \\
\underline{-3x^3+3x^2+12x-12} & \leftarrow \cdot -3 & \\
6x^2-18x+12 & & \\
x^2-3x+2 & & \\
 & \underline{x^3-3x+2} & \leftarrow \cdot 1 \\
 & -x^2-x+2 & \\
 & \cdot -x \rightarrow & \underline{x^3+x^2-2x} \\
 & & \underline{\underline{-x^2-x+2}} \\
\underline{x^2+x-2} & \leftarrow \cdot -1 & \\
-4x+4 & & \\
x-1 & & \\
\cdot -x \rightarrow & \underline{-x^2+x} & \\
 & -2x+2 & \\
 & \underline{\underline{x-1}} &
\end{array}$$

leaving just $\left\langle x-1 \right\rangle$.

22.

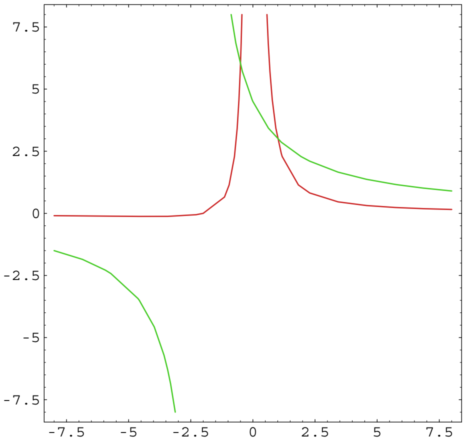
$$\begin{array}{cc}
x^5+x^2+2x-5 & x^3-x^2+x-1 \\
\underline{x^5-x^4+x^3-x^2} & \leftarrow\cdot x^2 \\
x^4-x^3+2x^2+2x-5 & \\
\underline{x^4-x^3+x^2-x} & \leftarrow\cdot x \\
x^2+3x-5 & \\
\cdot x\rightarrow & \underline{x^3+3x^2-5x} \\
 & -4x^2+6x-1 \\
\cdot-4\rightarrow & \underline{-4x^2-12x+20} \\
 & 18x-21 \\
 & 6x-7 \\
\underline{x^2-\frac{7}{6}x} & \leftarrow\cdot\frac{1}{6}x \\
\frac{25}{6}x-5 & \\
\cdot\frac{36}{25}\rightarrow & \underline{6x-\frac{36}{5}} \\
 & \frac{1}{5}
\end{array}$$

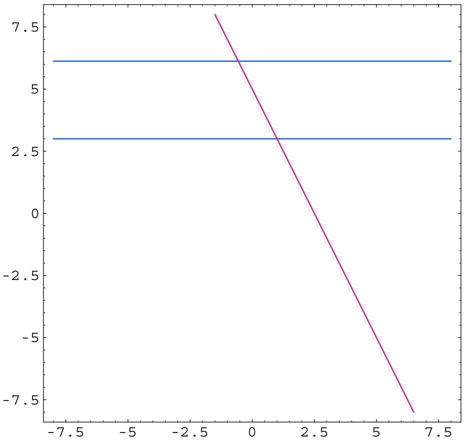
leaving $\langle 1\rangle$.

23.

$$\begin{array}{cc}
x^2y-x-2 & xy+2y-9 \\
\underline{x^2y+2xy-9x} & \leftarrow\cdot x \\
-2xy+8x-2 & \\
xy-4x+1 & \\
\cdot 1\rightarrow & \underline{xy-4x+1} \\
 & 4x+2y-10 \\
 & 2x+y-5 \\
\underline{xy+\frac{1}{2}y^2-\frac{5}{2}y} & \leftarrow\cdot-2 \\
-4x-\frac{1}{2}y^2+\frac{5}{2}y+1 & \\
\underline{-4x-2y+10} & \leftarrow\cdot-2 \\
-\frac{1}{2}y^2+\frac{9}{2}y-9 & \\
y^2-9y+18 &
\end{array}$$

y has zeros $y=\dfrac{+9\pm\sqrt{9^2-4\cdot 1\cdot 18}}{2\cdot 1}=\dfrac{9\pm\sqrt{81-72}}{2}=\dfrac{9\pm\sqrt{9}}{2}=\dfrac{9\pm 3}{2}=3,6$ and from $2x+y-5=0 \quad\Rightarrow 2x=-y+5 \quad\Rightarrow x=\frac{1}{2}\left(-y+5\right)$ the corresponding algebraic variety is $\left\{\left(1,3\right),\left(-\frac{1}{2},6\right)\right\}$. In the left figure are plotted the zeros of the two original polynomials, in the right figure the zeros of the corresponding Gröbner basis. Again, the common zeros of the Gröbner basis are the same as those of the original, but the basis is as simple as it could possibly be.





24. $x^2y + x \quad xy^2 - y$

$$\begin{aligned} S_{12} &= y\left(x^2y + x\right) - x\left(xy^2 - y\right)\\ &= x^2y^2 + xy - x^2y^2 + xy\\ &= 2xy \end{aligned}$$

$$\begin{array}{lll} \underline{x^2y} & & \leftarrow \cdot \tfrac{1}{2}x\\ x & & \\ & \underline{xy^2} & \leftarrow \cdot \tfrac{1}{2}y\\ & -y & \\ \cdot 2y \rightarrow & & \underline{2xy}\\ & y & \underline{\underline{0}} \end{array}$$

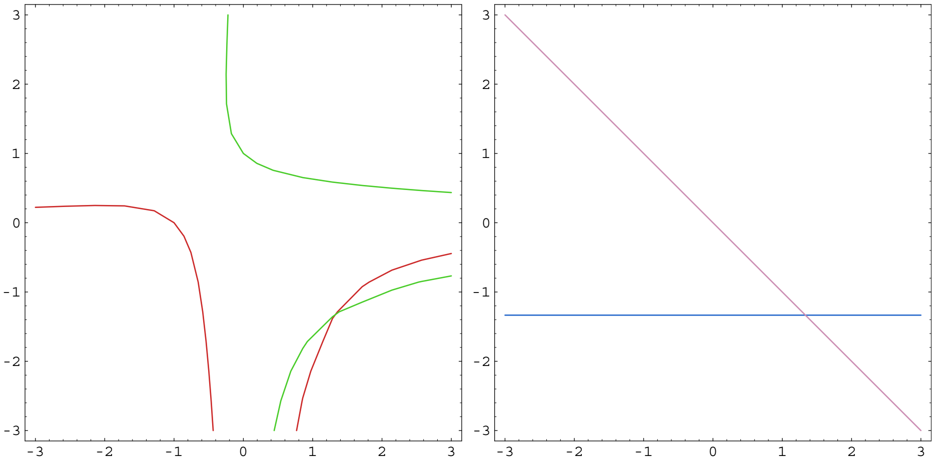
leaving $\langle x, y\rangle$ which is obviously a Gröbner basis. The corresponding algebraic variety is $\{(0,0)\}$.

25. $x^2y + x + 1 \quad xy^2 + y - 1$

$$\begin{aligned} S_{12} &= y\left(x^2y + x + 1\right) - x\left(xy^2 + y - 1\right)\\ &= x^2y^2 + xy + y - x^2y^2 - xy + x\\ &= x + y \end{aligned}$$

$$\begin{array}{lll} \underline{x^2y + xy^2} & & \leftarrow \cdot xy\\ -xy^2 + x + 1 & & \\ \underline{-xy^2 - y^3} & & \leftarrow \cdot -y^2\\ x + y^3 + 1 & & \\ \underline{x + y} & & \leftarrow \cdot 1\\ y^3 - y + 1 & & \\ & \underline{xy^2 + y^3} & \leftarrow \cdot y^2\\ & -y^3 + y - 1 & \\ & \underline{\underline{y^3 - y + 1}} & \end{array}$$

leaving $\langle y^3 - y + 1, x + y\rangle$.



26.

$$\begin{array}{ll} x^2y + xy^2 & xy - x \\ \underline{x^2y - x^2} & \leftarrow \cdot x \\ x^2 + xy^2 & \\ \underline{xy^2 - xy} & \leftarrow \cdot y \\ x^2 + xy & \\ \underline{xy - x} & \leftarrow \cdot 1 \\ x^2 + x & \end{array}$$

$$\begin{aligned} S_{12} &= y\left(x^2 + xy^2\right) - x\left(xy - x\right) \\ &= x^2y + xy^3 - x^2y + x^2 \\ &= xy^3 + x^2 \end{aligned}$$

$$\begin{array}{rl} \cdot y^2 \rightarrow & \underline{xy^3 - xy^2} \\ & x^2 + xy^2 \\ \cdot 1 \rightarrow & \underline{x^2 + xy^2} \\ & \underline{\underline{0}} \end{array}$$

leaving $\left\langle x^2 + x, xy - x \right\rangle$.

27. a. true (Theorem 5, the Hilbert Basis Theorem)

b. false (a fractal for example has infinite complexity, or $\mathbb{Z} \times \mathbb{Z}$ has infinitely many disjoint subsets, and neither can be described by a finite-basis ideal)

c. true ($\mathrm{V}\left\langle 1 \right\rangle$)

d. true (every point in $\mathbb{R}^2$ is the intersection of $\mathbb{R}^2$ and a line perpendicular to $\mathbb{R}^2$)

e. true (corresponding to the intersection of two planes in $\mathbb{R}^3$)

f. true (every line is the intersection of $\mathbb{R}^2$ and a plane perpendicular to $\mathbb{R}^2$ in $\mathbb{R}^3$)

g. true

h. true (finding solutions to systems of linear equations)

i. false

j. false (the algebraic variety is only a property of the basis, not the basis itself— notably, $x \in \left\langle x, y \right\rangle$ but $x \notin \left\langle x^2, y^2 \right\rangle$)

28. $y < x$ but $y \neq_x 0$.

29. $\forall +_i\, c_i f_i \in I: \quad \forall r \in R: \quad r\left(+_i\, c_i f_i\right) = +_i\, r c_i f_i = +_i\, c_i' f_i \in I$ where $c_i' = r c_i$. ¿So why does the ring need to be commutative with unity?

30. $\Rightarrow$Let $s \in F\left[\mathbf{x}\right]$ be a common divisor of f and g, $f = sf'$, $g = sg'$. Then

$f = gq + r \quad \Rightarrow r = f - gq = sf' - sg'q = s\left(f' - g'q\right)$ so s is also a divisor of r.

$\Leftarrow$Let $s \in F[\mathbf{x}]$ be a common divisor of g and r, $g = sg'$, $r = sr'$. Then $f = gq + r = sg'q + sr' = s(gq' + r')$ so s is also a divisor of f.

31. $xy \quad y^2 - y$

$$\begin{aligned} S &= y(xy) - x(y^2 - y) \\ &= xy^2 - xy^2 + y = y \end{aligned}$$

$\underline{xy} \qquad \leftarrow \cdot x$

$\underline{\underline{0}}$

$\underline{y^2} \qquad \leftarrow \cdot y$

$-y$

$\underline{-y} \qquad \leftarrow \cdot -1$

$\underline{\underline{0}}$

Since the only possible S is reducible to 0, the given basis must be a Gröbner basis.

32. First, show that $I_S = \left\{_{f \in F[\mathbf{x}]} f \middle| \forall \mathbf{s} \in S : f\mathbf{s} = 0\right\} \subseteq F[\mathbf{x}]$ is a subring:

- (additive identity) $0_{F[\mathbf{x}]}: \quad \forall \mathbf{s} \in S: \quad 0_{F[\mathbf{x}]}\mathbf{s} = 0 \quad \Rightarrow 0_{F[\mathbf{x}]} \in I_S$;
- (additive inverse) $\forall f \in I_S: \quad \forall \mathbf{s} \in S: \quad (-f)\mathbf{s} = -(f\mathbf{s}) = -0 = 0 \quad \Rightarrow -f \in I_S$;
- (additive closure) $\forall f, g \in I_S: \quad \forall \mathbf{s} \in S: \quad (f + g)\mathbf{s} = f\mathbf{s} + g\mathbf{s} = 0 + 0 = 0 \quad \Rightarrow f + g \in I_S$;
- (multiplicative closure) $\forall f, g \in I_S: \quad \forall \mathbf{s} \in S: \quad (fg)\mathbf{s} = f\mathbf{s} \cdot g\mathbf{s} = 0 \cdot 0 = 0 \quad \Rightarrow fg \in I_S$.

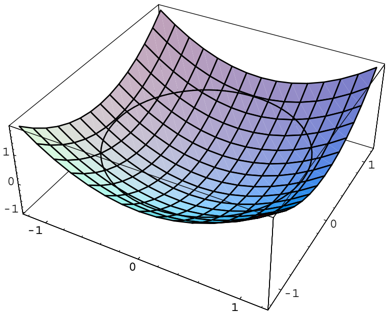
Next, show that $I_S \triangleleft F[\mathbf{x}]$:

$\forall f \in I_S: \quad \forall g \in F[\mathbf{x}]: \quad \forall s \in S: \quad (fg)\mathbf{s} = f\mathbf{s} \cdot g\mathbf{s} = 0 \cdot g\mathbf{s} = 0 \quad \Rightarrow fg \in I_S$.

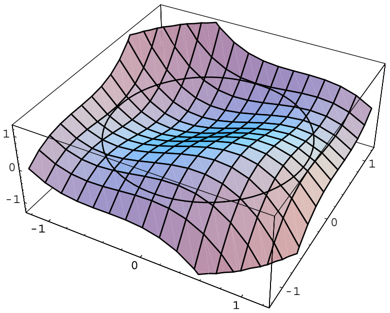
33. $\forall \mathbf{x} \in F^n: \quad \mathbf{x} \in \mathrm{V}\, I_S: \quad \Rightarrow \forall f \in I_S: \quad f\mathbf{x} = 0$ and this is obviously true by definition for all $\mathbf{s} \in S$, so $S \subseteq \mathrm{V}\, I_S$.

34. Let $S = \left\{_{x,y \in \mathbb{R}} (x, y) \middle| x^2 + y^2 = 1\right\} \setminus \{(1, 0)\}$ be the unit circle about the origin except for the single point on the positive x-axis. Then I_S is the ideal generated by $x^2 + y^2 - 1$ of all polynomials intersecting that circle. Because of the continuity of $\mathbb{R}$, obviously $(1, 0) \in \mathrm{V}\, I_S$.

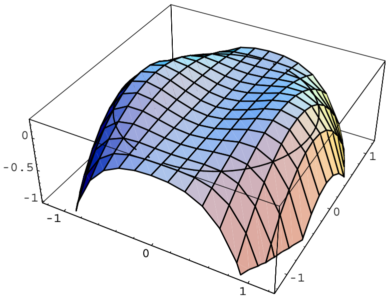
The following figures demonstrate some elements (polynomials) in that ideal and how they each intersect the unit circle:



$x^2 + y^2 - 1$



$(x^2 + y^2 - 1)(y - x)$



$(x^2 + y^2 - 1)(-x^2)$

35. Obviously any polynomial in N is zero-valued for any element of $\mathrm{V}N$, so $N \subseteq I_{\mathrm{V}\,N}$.

36. Let $N = \langle x^2 \rangle$, so N is every polynomial in $\mathbb{R}[x, y]$ in which every term is divisible by x^2. Obviously the y–axis $\left\{_{y \in \mathbb{R}} (0, y)\right\} \subseteq \mathrm{V}\, N$. Also, any point (a, b) not on the y-axis cannot be in $\mathrm{V}N$ because $x^2 \in N$ and $\phi_{(a,b)} x^2 = a^2 \neq 0$, so $\mathrm{V}\,N$ is precisely the y-axis. Now $I_{\mathrm{V}\,N}$ are all the polynomials that are zero-valued for the y-axis, which obviously

includes N. But also $x \in I_{\text{V N}}$ and $x \notin \left\langle x^2 \right\rangle$.

§7.1 Unique Factorization Domains

♥ By definition, a reducible can be factored into irreducibles but not vice versa. The key characteristic of a Prinicpal Ideal Domain is that every element can be identified with an ideal. Since the infinite union of an infinite sequence of properly contained ideals is $\langle 1 \rangle$, this terminates the sequence of ideals, and correspondingly therefore every element has a finite factorization. In a Prinicpal Ideal Domain an irreducible is prime, so the factorization is unique.

♥ 7

$$\begin{tikzcd}
D\text{ PID} \arrow[r, "7.1.16"] & D\text{ UFD} \arrow[d, "7.1.28"] \\
F[x]\text{ PID} \arrow[r] & D[x]\text{ UFD} \\
F\text{ field} \arrow[u, "6.2.24"] \arrow[uur, dashed, bend right] \arrow[ur, dotted, dash, bend right, "5.6.20"'] &
\end{tikzcd}$$

♥ 28

$$\begin{tikzcd}
D\text{ UFD} \arrow[d] & D[x]\text{ UFD} \\
F\text{ field of quotients} \arrow[r, "5.6.20"] & F[x]\text{ UFD} \arrow[u, "\text{recover a factorization of } f \in D[x] \text{ from one in } F[x]"']
\end{tikzcd}$$

1. Since 5 is prime, the only factorization up to associates of $5 \in \mathbb{Z}$ is $5 = 1 \cdot 5$ where 1 is a unit, so 5 is irreducible.
2. Since 17 is prime, the only factorization up to associates of $-17 \in \mathbb{Z}$ is $-17 = -1 \cdot 17$ where -1 is a unit, so -17 is irreducible.
3. $14 = 2 \cdot 7$ is reducible.
4. Is a primitive polynomial and irreducible.
5. $2x - 10 = 2(x - 5)$ is reducible.
6. $2x - 3$ is of degree 1 and $\forall a \neq 0 : 2x - 3 = \dfrac{2x-3}{a} \cdot a$ where a is a unit, so irreducible.
7. Idem, irreducible.
8. Irreducible.
9. $\mathbb{Z}[x]$: $\{2x - 7, -2x + 7\}$

   $\mathbb{Q}[x]$: $\{2x - 7, 4x - 14, 6x - 21, 8x - 28\}$

   $\mathbb{Z}_{11}[x]$: $\{2x - 7, 4x - 3, 6x + 1, 10x - 2\}$
10. The roots of the polynomial are

$$x = \frac{-(-4) \pm \sqrt{(-4)^2 - 4 \cdot 4 \cdot 8}}{2 \cdot 4} = \frac{4 \pm \sqrt{16 - 128}}{8} = \frac{4 \pm \sqrt{-112}}{8} = \frac{4 \pm 4\sqrt{7}}{8} = \tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{-7} \notin \mathbb{R}.$$

So in $\mathbb{Z}[x]$: $2 \cdot 2 \cdot (x^2 - x + 2)$, in $\mathbb{Q}[x]$: $4x^2 - 4x + 8$. In $\mathbb{Z}_{11}$ the polynomial has roots $x = 5, 7$ so in $\mathbb{Z}_{11}[x]$: $2 \cdot 2 \cdot (x - 5)(x - 7)$.

11. $$\left.\begin{aligned} 234 &= 2^1 \cdot 3^2 \cdot 13^1 \\ 3250 &= 2^1 \cdot 5^3 \cdot 13^1 \\ 1690 &= 2^1 \cdot 5^1 \cdot 13^2 \end{aligned}\right\} \Rightarrow \gcd = 2^1 \cdot 13^1 = 26$$

12. $$\left.\begin{aligned} 784 &= 2^4 \cdot 7^2 \\ 1960 &= 2^3 \cdot 5^1 \cdot 7^2 \\ 448 &= 2^6 \cdot 7^1 \end{aligned}\right\} \Rightarrow \gcd = 2^3 \cdot 7^1 = 56$$

13. $$\left.\begin{aligned} 2178 &= 2^1 \cdot 3^2 \cdot 11^2 \\ 396 &= 2^2 \cdot 3^2 \cdot 11^1 \\ 792 &= 2^3 \cdot 3^2 \cdot 11^1 \\ 594 &= 2^1 \cdot 3^3 \cdot 11^1 \end{aligned}\right\} \Rightarrow \gcd = 2^1 \cdot 3^2 \cdot 11^1 = 198$$

14. $6 \cdot \left(3x^2 - 2x + 8\right)$.

15. $18x^2 - 12x + 48$.

16. $2x^2 - 3x + 6$.

17. $2x^2 - 3x + 6$.

18. $a/b = ab^{-1}$ is only well-defined if *b* has an inverse. But even elements without an inverse can be associates, e.g. $26 = -26 \cdot -1$. So "if and only if $a = bu$, where *u* is a unit."

19. Insert "without one of the factors being a unit."

20. "Smaller" is not defined. "if and only if any divisor divides at least one of the factors in any factorization."

21.
a. true (a field does not have any nonzero nonunit elements)
b. true (by Corollary 6.2.6 a field has only the trivial and nonproper ideals, which are both principal)
c. true (Theorem 16)
d. false (Example 30)
e. true (by Corollary 17 $\mathbb{Z}$ is a UFD, and by Theorem 28 $\mathbb{Z}[x]$ is also)
f. false ($5, 7 \in \mathbb{Z}$ are irreducible but not associates)
g. false ($\mathbb{Z}[x]$ is a PID but $\mathbb{Z}[x][y] = \mathbb{Z}[x, y]$ is not)
h. true (Theorem 28)
i. false (an associate of *p* could appear)
j. true (by Definition 5 a UFD is only defined for an integral domain, which cannot have divisors of zero)

22. By Lemma 26. The irreducibles of $D[x]$ are the irreducibles of *D* and the irreducibles in $F[x]$ that are primitive in $D[x]$.

23. Again following Lemma 26, a nonprimitive polynomial in $D[x]$ is reducible in $F[x]$ but irreducible in $D[x]$, for example $2x + 2 = 2 \cdot (x + 1)$ is reducible in $\mathbb{Z}[x]$ but irreducible in $\mathbb{Q}[x]$.

24. With divisors of zero, factorizations are no longer unique. For example, $(1, 0) = (1, 0) \cdot (1, 3) = (1, 0) \cdot (1, 5)$.

25. Suppose $p = ab$ is reducible where a, b are not units. Then $a, b \neq_p 0$ are not divisible by *p*, for suppose without loss of generality that $a =_p 0$ then $a =_{ab} 0 \Rightarrow \exists c : a = abc$. Since an integral domain has no divisors of zero and $p \neq 0$, then $a \neq 0$. Since cancellation holds in an integral domain we have $1 = bc \Rightarrow c = b^{-1}$ but *b* is not a unit. So *p* is not prime. So if *p* is prime, it is irreducible.

26. Let $p = ab$ be a factorization of an irreducible *p*. Then without loss of generality, *a* is a unit. Since this factorization is unique up to associates and $ab =_p 0 \Rightarrow b =_p 0$, so *p* is prime.

27. • (reflexive) $a = a \cdot 1$ so $a \sim a$;

- (symmetric) $\forall a,b \in D : a \sim b \quad \Rightarrow \exists u \in D : a = bu \quad \Rightarrow b = au^{-1} \quad \Rightarrow b \sim a$, where u, u^{-1} are units;
- (transitive) $\forall a,b,c \in D : a \sim b, b \sim c \quad \Rightarrow \exists u,v \in D : a = bu, b = cv \quad \Rightarrow a = bu = (cv)u = c(vu) \quad \Rightarrow a \sim c$, where vu is also a unit.

28. Let $a,b \in D^* - U$ be two nonzero nonunits. Since D is an integral domain, it has no divisors of zero so $ab \neq 0$. Suppose ab was a unit, then $(ab)\cdot(ab)^{-1} = 1 \quad \Rightarrow a\left(b(ab)^{-1}\right) = 1 \quad \Rightarrow a^{-1} = b \cdot (ab)^{-1}$ and a would be a unit. So $D^* - U$ is closed. It is not a group because it does not contain the identity 1.

29. Let $f \in D[x]$ be primitive, and let $g,h \in D[x] : f = gh$. Suppose $g = cg'$ is not primitive. Because $D[x]$ is a UFD, $f = cg'h$ and f is thus not primitive.

30. Lemma 9 shows that every principal ideal is contained in a finite chain of ideals that terminates in $D = \langle 1 \rangle$.

31. $x^3 - y^3$ has a root for $x = y$, so $x^3 - y^3 = (x-y)\cdot(x^2 + xy + y^2)$. The quotient has roots $x = \dfrac{-y \pm \sqrt{y^2 - 4\cdot 1 \cdot y^2}}{2 \cdot 1} = \dfrac{-y \pm \sqrt{-3y^2}}{2} = \dfrac{-y \pm y\sqrt{-3}}{2}$ that are not in $\mathbb{Q}$.

32. • ACC ⇒ MC
By ACC, any chain of strictly increasing ideals is finite, therefore there is a last ideal in this chain that is not properly contained in any other ideal.
• $(\text{MC} \Rightarrow \text{FBC}) \Leftarrow (\overline{\text{FBC}} \Rightarrow \overline{\text{MC}})$
Suppose there is an ideal N that has no finite basis set. Surely it has at least an infinite one. Then we can construct an infinite set of ideals by iteratively adjoining one element from theis basis set, with each new ideal containing the pervious ideal. This set therefore does not satsify MC.
• FBC ⇒ ACC
If every ideal has a finite basis, then we can construct a finite chain of ideals by iteratively adjoining an element from the basis set to the previous ideal. Since every ideal in any chain can be constructed from a finite chain of ideals, the chain must be of finite length. (shaky…)

33. • $(\text{DCC} \Rightarrow \text{mC}) \Leftarrow (\overline{\text{mC}} \Rightarrow \overline{\text{DCC}})$
Suppose S was a set of ideals in which every ideal contains some other ideal of S. Then an infinitely long decreasing sequence of ideals would exist.
• mC ⇒ DCC
If any strictly decreasing sequence of ideals has an ideal that does not properly contain any other ideal in that sequence, the sequence must be finite.

34. ACC holds in $\mathbb{Z}$, but for any finite-basis ideal $\langle n \rangle \lhd \mathbb{Z}$ there is always another relative prime that can be adjoined to the basis to construct a new ideal properly contained in it.

§7.2 Euclidean Domains

♥ The valuation gives a measure by which we can guarantee that a factorization will at some point terminate.

♥ 9 Let D be a Euclidean domain with valuation v. Then for $r_0, r_1 \in D^*$:

$$\begin{aligned} r_0 &= r_1 q_2 + r_2 & r_2 &= 0 \vee vr_2 < vr_1 \\ r_1 &= r_2 q_3 + r_3 & r_3 &= 0 \vee vr_3 < vr_2 \\ &\vdots \\ r_{i-1} &= r_i q_{i+1} + r_{i+1} & r_{i+1} &= 0 \vee vr_{i+1} < vr_i \end{aligned}$$

If $r_{i-1} =_d 0, r_i =_d 0 \quad \Rightarrow r_{i+1} = r_{i-1} - r_i q_{i+1} =_d 0$ and if $r_{i+1} =_d 0, r_i =_d 0 \quad \Rightarrow r_{i-1} = r_i q_{i+1} + r_{i+1} =_d 0$, so the common divisors of r_{i-1}, r_i are the same as those of r_i, r_{i+1}. So when r_s is the first remainder equal to zero, a greatest common divisor of r_{s-2}, r_{s-1} is also one of r_0 and r_1. And since $r_{s-2} = r_{s-1}q_s + r_s = r_{s-1}q_s$, a greatesst common divisor of r_{s-2}, r_{s-1} is r_{s-1}.

1. On $\mathbb{Z}$, the q and r of Condition 1 do exist by Theorem 1.5.3 and $0 \le r < b$. From $r < b$ and $r, b \ge 0$ we have

$r^2 < b^2 \Rightarrow vr < vb$. Then $\forall a,b \in D^*: \quad a^2 \le (ab)^2 = a^2b^2 \quad \Leftarrow 1 \le b \quad \Leftarrow b \ge 1$.

2. We know by Theorem 5.6.1 that on the ring of polynomials over a field the quotient and remainder q and r in $a = bq + r$ are unique, so a solution may not exist in $\mathbb{Z}[x]$ and Condition 1 is not satisfied. For example, $(2x-1) = (2)\cdot\left(x - \tfrac{1}{2}\right) + (0)$.

3. Again, the quotient and remainder are unique but if the remainder is nonzero we cannot guarantee that $vr < vb$ and satisfy Condition 1. For example, $(1x+7) = (1x)\cdot(1) + (7)$ where $v7 \not< v(1x) \quad \Leftarrow 7 \not< 1$. The problem is that the process of division does not necessarily reduce v.

4. In a field, for any $a,b \in F$, $b \ne 0$, $a = bq$ always has a solution so Condition 1 is satisfied. But in $\mathbb{Q}$, for $0 < b < 1$ and any $a \in \mathbb{Q}^*$: $va \not\le v(ab) \quad \Leftarrow v(ab) < va \quad \Leftarrow a^2b^2 = (ab)^2 < a^2 \quad \Leftarrow b^2 < 1 \quad \Leftarrow 0 < b < 1$.

5. From Exercise 4, Condition 1 is satisfied. Also, $\forall a,b \in \mathbb{Q}^*: \; va = v(ab)$.

6.
$$\begin{aligned}23 &= 3\cdot 138 - 391\\ &= 3\cdot(3266 - 391\cdot 8) - 391 = 3\cdot 3266 - 24\cdot 391 = 3\cdot 3266 - 25\cdot 391\\ &= 3\cdot 3266 - 25\cdot(7\cdot 3266 - 1\cdot 22471) = 3\cdot 3266 - 175\cdot 3266 + 25\cdot 22471\\ &= -172\cdot 3266 + 25\cdot 22471\end{aligned}$$

7.
$$\left.\begin{aligned}49349 &= 15555\cdot 3 + 2684\\ 15555 &= 2684\cdot 6 - 549\\ 2684 &= 549\cdot 5 - 61\\ 549 &= 61\cdot 9\end{aligned}\right\} \Rightarrow \gcd(49349, 15555) = 61$$

8.
$$\begin{aligned}61 &= 5\cdot 549 - 1\cdot 2684\\ &= 5\cdot(6\cdot 2684 - 1\cdot 15555) - 1\cdot 2684 = 29\cdot 2684 - 5\cdot 15555\\ &= 29\cdot(1\cdot 49349 - 3\cdot 15555) - 5\cdot 15555 = 29\cdot 29349 - 92\cdot 15555\end{aligned}$$

9. By polynomial long division:

$$\begin{aligned}&\left(x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3\right)\\ &\qquad = \left(x^4 - 2x\right)\cdot\left(x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2\right) + \left(-x^4 - 3x^3 - 2x^2 - 5x + 3\right)\end{aligned}$$

$$\left(x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2\right) = \left(-x^2 + 6x - 19\right)\cdot\left(-x^4 - 3x^3 - 2x^2 - 5x + 3\right) + \left(-59x^3 - 118x + 59\right)$$

$$\left(-x^4 - 3x^3 - 2x^2 - 5x + 3\right) = \left(\tfrac{1}{59}x + \tfrac{3}{59}\right)\cdot\left(-59x^3 - 118x + 59\right)$$

so $59\cdot\left(-x^3 - 2x + 1\right)$ and $x^3 + 2x - 1$ are greatest common divisors.

10. Calculate $d_{i+1} = \gcd(a_i, d_i)$, where $d_0 = a_0$.

11.
$$\begin{aligned}2178 &= 396\cdot 5 + 198 &&\\ 396 &= 198\cdot 2 && d_1 = \gcd(2178, 396) = 198\\ 792 &= 198\cdot 4 && d_2 = \gcd(792, 198) = 198\\ 726 &= 198\cdot 4 - 66 &&\\ 198 &= 66\cdot 3 && d_3 = \gcd(726, 198) = 66\end{aligned}$$

12. a. Yes, because $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Arithmetic and $\mathbb{Z}[x]$ is a UFD by Theorem 1.28.

b. This is the subset of $\mathbb{Z}[x]$ with even constant term. It is fairly obvious that it is in fact closed and a subring. Now consider any $g \in \mathbb{Z}[x]: g = xg' + (g_0 + 1), \quad g' \in \mathbb{Z}[x], g_0 \in 2\mathbb{Z}$ polynomial with odd constant term and any $f = xf' + f_0, \quad f' \in \mathbb{Z}[x], f_0 \in 2\mathbb{Z}$ in the subring. Then

$$\begin{aligned} f \cdot g &= \left(xg' + \left(g_0 + 1\right)\right) \cdot \left(xf' + f_0\right) \\ &= x^2 f'g' + f_0 xg' + \left(g_0 + 1\right)xf' + \left(g_0 + 1\right)f_0 \\ &= x^2 f'g' + \left(f_0 g' + \left(g_0 + 1\right)f'\right)x + \left(g_0 f_0 + f_0\right) \end{aligned}$$

It is obvious that the constant term $g_0 f_0 + f_0$ is again even, so the subring is indeed ideal.

c. No. Any generator of the ideal in (b.) would have to have even constant term, but this wouldn't then generate polynomials with odd coefficients on nonconstant terms. For example, there is no polynomial that will generate both 2 and x.

d. No, by Theorem 4.

13. a. true (Theorem 4)
b. false (by the discussion after Corollary 5)
c. true (Corollary 5)
d. false (by the discussion after Corollary 5 and Exercise 12)
e. true (in a field, every nonzero element is a greatest common divisor of any set of nonzero elements)
f. true
g. true (Theorem 6)
h. false (by Theorem 6 every unit u has $\nu u = \nu 1$, not only the multiplicative identity)
i. true (Theorem 6)
j. true (Example 3)

14. No, because the arithmetic structure of a domain D is defined by its operations and is independent of any particular choice of valuation.

15. If a and b are associates then there exists a unit u such that $a = bu$. By Condition 2 of Definition 1, $\nu a = \nu\left(bu\right) \le \nu\left(bu \cdot u^{-1}\right) = \nu b$, and conversely, so $\nu a = \nu b$.

16. If b is a unit, then a and ab are associates and by Exercise 15 $\nu a = \nu\left(ab\right)$. Conversely …

17. This is the set of all elements with valuation greater than that of a unit. Condition 2 shows that the set is closed under multiplication, but it is not closed under addition and hence not a group. For example, for $3, -2 \in \mathbb{Z}$, $\nu 3, \nu\left(-2\right) > 1$ and $\nu\left(3 + \left(-1\right)\right) = \nu 1$.

18. In any field, Condition 1 holds with zero remainder always. If ν is the identity $i\big|_{D^*}$, Condition 2 holds as well.

19. a. Since ν is minimal for $\nu 1$, η has minimum value $\eta 1 = \nu 1 + s > 0$, so $\eta : D^* \to \mathbb{Z}^+$. Also, if Condition 1 holds for ν then it also holds for η because $\eta r < \eta b \Leftarrow \nu r < \nu b$, and if Condition 2 holds for ν it also holds for η because $\eta a \le \eta\left(ab\right) \Leftarrow \nu a \le \nu\left(ab\right)$.

b. Since ν is minimal for $\nu 1$ and $r > 0$, l has minimum value $r \cdot \nu 1 \ge 0$, and since ν maps to integers and $r \in \mathbb{Z}^+$, $\lambda : D^* \to \mathbb{Z}^+$. If Condition 1 holds for ν then it also holds for λ because $\lambda r < \lambda b \Leftarrow \nu r < \nu b$, and if Condition 2 holds for ν it also holds for λ because $\lambda a \le \lambda\left(ab\right) \Leftarrow \nu a \le \nu\left(ab\right)$.

c. Let ν be any valuation. Then $\mu : D^* \to \mathbb{Z}^+ : a \mapsto \left(\nu a - \nu 1\right) \cdot 100 + 1$ is a Euclidean valuation by (a.) and (b.), with $\mu 1 = \left(\nu 1 - \nu 1\right) \cdot 100 + 1 = 1$. Since ν has minimum value $\nu 1$, $\nu a \ge \nu 1 + 1$ for any nonzero nonunit, and $\mu a \ge \left(\left(\nu 1 + 1\right) - \nu 1\right) \cdot 100 + 1 = 101 > 100$.

20. For any $a, b \in D^*$, $\langle a \rangle, \langle b \rangle$ are their principal ideals, that is, all their multiples. Then $\langle a \rangle \cap \langle b \rangle$ is an ideal by Exercise 6.1.27 of all the common multiples of a and b. Since D is a Euclidean domain it is a PID, so $\exists c \in D : \langle a \rangle \cap \langle b \rangle = \langle c \rangle$. Since $ab \ne 0$ and $ab \in \langle c \rangle$ we know that $\langle c \rangle \ne E$ and $c \ne 0$. Since c divides every element of $\langle c \rangle$, it is a least common multiple.

21. If a and b are relatively prime, then by Theorem 9 $\exists \lambda, \mu \in D : \lambda a + \mu b = \gcd\left(a, b\right) = 1$, so a and b generate $\langle 1 \rangle = \mathbb{Z}$.

Conversely, let $d = \gcd(a,b)$. Every element generated by a and b is of the form $\lambda a + \mu b = d\left(\frac{\lambda a}{d} + \frac{\mu b}{d}\right) \supseteq \langle d \rangle$, so to generate $\mathbb{Z}$ we must have $d = 1$, which is to say that a and b must be relatively prime.

22. If a and n are relatively prime, then by Theorem 9 $\exists \lambda, \mu \in \mathbb{Z}$:

$$\lambda a + \mu n = 1 \quad \Rightarrow b(\lambda a + \mu n) = b \quad \Rightarrow (b\lambda)a + (b\mu)n = b \quad \Rightarrow (b\lambda)a =_n b \quad \Rightarrow x = b\lambda.$$

23. Let $d = \gcd(a,n)$. By Theorem 9 $\exists \lambda, \mu \in \mathbb{Z} : \lambda a + \mu n = d$. Since d divides b, $\exists \alpha \in \mathbb{Z} : b = \alpha d$. Then $\alpha(\lambda a + \mu n) = \alpha d = b \quad \Rightarrow (\alpha\lambda)a + (\alpha\mu)n = b \quad \Rightarrow (\alpha\lambda)a =_n b \quad \Rightarrow x = \alpha\lambda$. Conversely, if $ax =_n b$ then $\exists \lambda \in \mathbb{Z} : ax + \lambda n = b$. Now $d = \gcd(a,n)$ obviously divides $ax + \lambda n$, so if it does not also divide b the equation cannot possibly have a solution. In other words, $ax = b$ has a solution for x in $\mathbb{Z}_n$ iff the greatest common divisor of a and n divides b.

24. Find λ by the procedure outlined in Exercise 6, and let $d = \gcd(a,n)$. Verify that d divides b, then $x = \alpha\lambda = \frac{\lambda b}{d}$. So $42 = 22 \cdot 2 - 2, \quad 22 = 2 \cdot 11$ so $d = \gcd(42,22) = 2$. We see that 2 indeed divides 18, so there is a solution $x = \frac{\lambda b}{d} = \frac{2 \cdot 18}{2} = 18$.

§7.3 Gaussian Integers and Norms

1. $a + bi \in \mathbb{C} : \frac{5}{a+bi} = \frac{5 \cdot (a - bi)}{(a+bi)(a-bi)} = \frac{5a - 5bi}{a^2 + b^2} = \frac{5 - 10i}{5} = 1 - 2i$, where $a = 1, b = 2$, so $5 = (1+2i)(1-2i)$.

2. $N7 = 49$ has to be factored into two factors, so we are looking for $a + bi$ with norm 7 but that doesn't exist by Theorem 10. Irreducible.

3. $\frac{4+3i}{a+bi} = \frac{(4+3i)(a-bi)}{(a+bi)(a-bi)} = \frac{(4a+3b)+(3a-4b)i}{a^2+b^2} = \frac{(4\cdot 1 + 3 \cdot 2) + (3 \cdot 1 - 4 \cdot 2)i}{1^2 + 2^2} = 2 - i$, where $a = 1, b = 2$, so $4 + 3i = (1+2i)(2-i)$.

4. $\frac{6-7i}{a+bi} = \frac{(6-7i)(a-bi)}{(a+bi)(a-bi)} = \frac{(6a-7b)+(-7a-6b)i}{a^2+b^2} = \frac{(6 \cdot 4 - 7 \cdot 1) + (-7 \cdot 4 - 6 \cdot 1)i}{1^2 + 4^2} = 1 - 2i$, where $a = 4, b = 1$, so $6 - 7i = (4+i)(1-2i)$.

5.
$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right) \end{aligned}$$

6. $\frac{\alpha}{\beta} = \frac{7+2i}{3-4i} = \frac{(7+2i)(3+4i)}{(3-4i)(3+4i)} = \frac{(21-8)+(28+6)i}{3^2+4^2} = \frac{13}{25} + \frac{34}{25}i \quad \Rightarrow \sigma = 1 + i$

$\rho = \alpha - \beta\sigma = (7+2i) - (3-4i)(1+i) = (7+2i) - ((3+4)+(3-4)i) = (7+2i) - (7-i) = i$.

7.
$$\begin{cases} \frac{8+6i}{5-15i} = \frac{(8+6i)(5+15i)}{(5-15i)(5+15i)} = \frac{(8 \cdot 5 - 6 \cdot 15) + (8 \cdot 15 + 6 \cdot 5)i}{5^2 + 15^2} = \frac{-50 + 150i}{250} = -\frac{1}{5} + \frac{3}{5}i \\ i \cdot (5 - 15i) = 15 + 5i \\ (8+6i) - (15+5i) = -7 + i \\ 8 + 6i = i \cdot (5 - 15i) + (-7 + i) \end{cases}$$

$$\begin{cases} \dfrac{5-15i}{-7+i} = \dfrac{(5-15i)(-7-i)}{7^2+1^2} = \dfrac{\left(5\cdot(-7)-(-15)\cdot(-1)\right)+\left(5\cdot(-1)+(-15)\cdot(-7)\right)i}{50} = \dfrac{-50+100i}{50} = -1+2i \\ 5-15i = (-1+2i)\cdot(-7+i) \end{cases}$$

$\gcd(8+6i, 5-15i) = -7+i$

8. a. true (Theorem 4 and Theorem 2.4)
b. true (Theorem 4)
c. true (Definition 1)
d. false ($\frac{1}{2} \notin \mathbb{Z}[i]$)
e. true (the Euclidean algorithm holds in any Euclidean domain, Theorem 9)
f. true (in the case of Theorem 7, a prime multiplicative norm corresponds to an irreducible)
g. true (Theorem 7)
h. false ($\deg 0 < 0$ so Condition 1 of Definition 6 doesn't hold, $\deg 1 = 0$ so Condition 2 doesn't hold, and $\deg x^2 \neq \deg x \cdot \deg x \Leftarrow 2 \neq 1 \cdot 1$ so Condition 3 doesn't hold either)
i. true (all three conditions of Definition 6 hold)
j. true (Example 9)

9. If $\pi \in D$ such that $N\pi$ is minimal, then if π was reducible there would be $\sigma, \rho \in D : \pi = \sigma\rho$ with neither σ, ρ a unit and thus $N\sigma, N\rho \neq 1$, but then either $N\sigma, N\rho < N\pi$ which is a contradiction. So π is irreducible.

10. a. $2 = -i \cdot 2i = -i \cdot (1+i)^2$.

b. By Theorem 10, $p =_4 1 \Rightarrow p = a^2 + b^2 = (a+bi)(a-bi)$ reducible in $\mathbb{Z}[i]$. Conversely, if $p =_4 3$ was reducible then $p = a \cdot b$ and $Np = p^2 = Na \cdot Nb \Rightarrow Na, Nb = p$ and $Na = p \Rightarrow N(a' + a''i) = a'^2 + a''^2 = p$ but there is no such expression by Theorem 10.

11. 1. $N\alpha = a'^2 + a''^2 \geq 0$, where $a', a'' \in \mathbb{Z}$.
2. $N\alpha = a'^2 + a''^2 = 0 \Leftrightarrow a'^2 = 0 \wedge a''^2 = 0 \Leftrightarrow a' = 0 \wedge a'' = 0 \Leftrightarrow a = 0$.
3. $N(\alpha\beta) = N\left((\alpha' + i\alpha'')\cdot(\beta' + i\beta'')\right) = N\left((\alpha'\beta' - \alpha''\beta'') + (\alpha'\beta'' + \alpha''\beta')i\right)$

$$\begin{aligned} &= (\alpha'\beta' - \alpha''\beta'')^2 + (\alpha'\beta'' + \alpha''\beta')^2 \\ &= (\alpha'\beta')^2 - 2\alpha'\alpha''\beta'\beta'' + (\alpha''\beta'')^2 + (\alpha'\beta'')^2 + 2\alpha'\alpha''\beta'\beta'' + (\alpha''\beta')^2 \\ &= (\alpha'^2 + \beta'^2)\cdot(\beta'^2 + \beta''^2) \\ &= N(\alpha' + i\alpha'')\cdot N(\beta' + i\beta'') = N\alpha \cdot N\beta \end{aligned}$$

12. $\forall \alpha = \alpha' + i\alpha''\sqrt{5}, \beta = \beta' + i\beta''\sqrt{5}$:

$$\begin{aligned} N(\alpha\beta) &= N\left(\left(\alpha' + i\alpha''\sqrt{5}\right)\cdot\left(\beta' + i\beta''\sqrt{5}\right)\right) = N\left((\alpha'\beta' - 5\alpha''\beta'') + (\alpha'\beta'' + \alpha''\beta')i\sqrt{5}\right) \\ &= (\alpha'\beta' - 5\alpha''\beta'')^2 + 5(\alpha'\beta'' + \alpha''\beta')^2 \\ &= (\alpha'\beta')^2 - 10\alpha'\alpha''\beta'\beta'' + 25\alpha''\beta'' + 5(\alpha'\beta'')^2 + 10\alpha'\alpha''\beta'\beta'' + 5(\alpha''\beta')^2 \\ &= (\alpha'^2 + 5\alpha''^2)\cdot(\beta'^2 + 5\beta''^2) \\ &= N\left(\alpha + i\alpha''\sqrt{5}\right)\cdot N\left(\beta' + i\beta''\sqrt{5}\right) = N\alpha \cdot N\beta \end{aligned}$$

13. Let d be a nonzero nonunit. Suppose $\exists a, b : d = ab$ where a, b nonunit. Because $Nd = Na \cdot Nb$ and $Na, Nb > 1$ it must be that $Na, Nb < Nd$. Otherwise, if $\nexists a, b : d = ab$ where a, b nonunit, d is irreducible. Because Nd has a finite factorization in $\mathbb{Z}$, repeating this procedure will at some point terminate.

14.

$$\begin{cases} \dfrac{16+7i}{10-5i} = \dfrac{(16+7i)(10+5i)}{(10-5i)(10+5i)} = \dfrac{(16\cdot 10 - 7\cdot 5)+(16\cdot 5 + 7\cdot 10)i}{125} = \dfrac{125+150i}{125} = 1+1\tfrac{1}{5}i \\ (1+i)(10-5i) = (10\cdot 1 - (-5)\cdot 1) + (10\cdot 1 - 5\cdot 1)i = 15+5i \\ (16+7i)-(15+5i) = 1+2i \\ 16+7i = (1+i)\cdot(10-5i)+(1+2i) \end{cases}$$

$$\begin{cases} \dfrac{10-5i}{1+2i} = \dfrac{(10-5i)(1-2i)}{(1+2i)(1-2i)} = \dfrac{(10\cdot 1 - 5\cdot 2)+(10\cdot(-2)+(-5)\cdot 1)i}{5} = \dfrac{-25i}{5} = -5i \end{cases}$$

$$\gcd(16+7i, 10-5i) = 1+2i$$

15. a. Since $\mathbb{Z}[i]$ is a Euclidean domain, there exists a valuation v on $\mathbb{Z}[i]$. Then $\forall \beta \in D : \exists \beta_0, \beta^* \in D : \beta = \beta^*\alpha + \beta_0$ where $\beta_0 = 0$ or $v\beta_0 < v\alpha$. So $\psi : \mathbb{Z}[i] \to \dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle} : \beta \mapsto \beta_0 + \langle\alpha\rangle$ is the canonical homomorphism onto $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$ and the conditions on β_0 show that there are a finite number of them.

b. If $\langle\pi\rangle$ were not maximal then there would be $\rho \notin \langle\pi\rangle : \langle\pi\rangle \subset \langle\rho\rangle \subset \mathbb{Z}[i]$ so $\exists\sigma : \pi = \rho\sigma$ where ρ not a unit (else $\langle\rho\rangle = \langle\pi\rangle$), but then π would be reducible. So $\langle\pi\rangle$ is maximal and $\mathbb{Z}[i]/\langle\pi\rangle$ a field.

c. I verified these by plotting on graph paper. The characteristic is pretty simple to find, the order seems always to be equal to the norm.

i. $\dfrac{\mathbb{Z}[i]}{\langle 3\rangle} = \left\{_{0\le\alpha',\alpha''<3} \quad \alpha' + i\alpha'' + \langle 3\rangle\right\}$. $\left|\dfrac{\mathbb{Z}[i]}{\langle 3\rangle}\right| = 9$; $\operatorname{char}\dfrac{\mathbb{Z}[i]}{\langle 3\rangle} = 3$;

ii. $\left|\dfrac{\mathbb{Z}[i]}{\langle 1+i\rangle}\right| = 2$; $\operatorname{char}\dfrac{\mathbb{Z}[i]}{\langle 1+i\rangle} = 2$;

iii. $\left|\dfrac{\mathbb{Z}[i]}{\langle 1+2i\rangle}\right| = 5$; $\operatorname{char}\dfrac{\mathbb{Z}[i]}{\langle 1+2i\rangle} = 5$.

16. I don't think n needs to be 'square free' in this exercise but in the next one.

a. Obviously $\forall\alpha \in \mathbb{Z}\left[\sqrt{-n}\right] : N\alpha \ge 0$. Also, $N\alpha = 0 \Leftrightarrow a^2 + nb^2 = 0 \Leftrightarrow a^2, b^2 = 0 \Leftrightarrow a, b = 0$. Finally,

$\forall\alpha,\beta \in \mathbb{Z}\left[\sqrt{-n}\right] : \alpha = \alpha' + i\alpha''\sqrt{n}, \beta = \beta' + i\beta''\sqrt{n} :$

$$\begin{aligned} N\alpha\beta &= N\left(\left(\alpha' + i\alpha''\sqrt{n}\right)\cdot\left(\beta' + i\beta''\sqrt{n}\right)\right) \\ &= N\left(\left(\alpha'\beta' - n\alpha''\beta''\right) + \left(\alpha'\beta'' + \alpha''\beta'\right)i\sqrt{n}\right) \\ &= \left(\alpha'\beta' - n\alpha''\beta''\right)^2 + n\left(\alpha'\beta'' + \alpha''\beta'\right)^2 \\ &= \left(\alpha'\beta'\right)^2 - 2n\alpha'\alpha''\beta'\beta'' + n^2\alpha''\beta'' + n\left(\alpha'\beta''\right)^2 + 2n\alpha'\alpha''\beta'\beta'' + n\left(\alpha''\beta'\right)^2 \\ &= \left(\alpha'^2 + n\alpha''^2\right)\left(\beta'^2 + n\beta''^2\right) \\ &= N\left(\alpha' + i\alpha''\sqrt{n}\right)\cdot N\left(\beta' + i\beta''\sqrt{n}\right) = N\alpha\cdot N\beta \end{aligned}$$

b. $\forall\alpha \in \mathbb{Z}\left[\sqrt{-n}\right] : N\alpha = 1 \quad \Rightarrow N\left(\alpha' + i\alpha''\sqrt{n}\right) = \alpha'^2 + n\alpha''^2 = 1 \quad \Rightarrow \begin{cases} \alpha'^2 = 1 \wedge n\alpha''^2 = 0 \\ \alpha'^2 = 0 \wedge n\alpha''^2 = 1 \end{cases} \quad \Rightarrow \begin{cases} \alpha' = \pm 1 \wedge \alpha'' = 0 \\ \alpha' = 0 \wedge \alpha'' = \pm 1 \wedge n = 1 \end{cases}$

Since these elements are also the only possible units, this describes precisely all the units.

c. We show that $\mathbb{Z}\left[\sqrt{-n}\right]$ is an integral domain by showing it has no divisors of zero:

$\alpha\beta = 0 \quad \Rightarrow N(\alpha\beta) = N\alpha \cdot N\beta = 0 \quad \Rightarrow N\alpha = 0 \vee N\beta = 0 \quad \Rightarrow \alpha = 0 \vee \beta = 0$

Then by Exercise 13 and (b.) every nonzero nonunit has a factorization into irreducibles.

17. I think n needs to be 'square free' in this exercise but not in the previous one.

a. Obviously $\forall\alpha \in \mathbb{Z}\left[\sqrt{n}\right] : N\alpha \geq 0$. Also, $\forall\alpha : N\alpha = 0 \Leftrightarrow \left|\alpha'^2 - n\alpha''^2\right| = 0 \Leftrightarrow \alpha'^2 = n\alpha''^2 \overset{*}{\Leftrightarrow} \alpha', \alpha'' = 0$, where (*) holds only if n is square free— for example, if $n = 3 : \alpha'^2 = 3\alpha''^2 \Leftrightarrow \alpha', \alpha'' = 0$ but if $n = 4$: $\alpha'^2 = 4\alpha''^2 \Leftarrow \alpha' = 2, \alpha'' = 1$. Then, $\forall\alpha, \beta \in \mathbb{Z}\left[\sqrt{n}\right]$:

$$\begin{aligned}
N(\alpha\beta) &= N\left(\left(\alpha' + \alpha''\sqrt{n}\right) \cdot \left(\beta' + \beta''\sqrt{n}\right)\right) \\
&= N\left(\left(\alpha'\beta' + n\alpha''\beta''\right) + \left(\alpha'\beta'' + \alpha''\beta'\right)\sqrt{n}\right) \\
&= \left|\left(\alpha'\beta' + n\alpha''\beta''\right)^2 - n\left(\alpha'\beta'' + \alpha''\beta'\right)^2\right| \\
&= \left|\left(\alpha'\beta'\right)^2 + 2n\alpha'\alpha''\beta'\beta'' + \left(n\alpha''\beta''\right)^2 - n\left(\alpha'\beta''\right)^2 - 2n\alpha'\alpha''\beta'\beta'' - n\left(\alpha''\beta'\right)^2\right| \\
&= \left|\left(\alpha'^2 - n\alpha''^2\right)\left(\beta'^2 - n\beta''^2\right)\right| \\
&= \left|\alpha'^2 - n\alpha''^2\right| \cdot \left|\beta'^2 - n\beta''^2\right| \\
&= N\left(\alpha' + \alpha''\sqrt{n}\right) \cdot N\left(\beta' + \beta''\sqrt{n}\right) = N\alpha \cdot N\beta
\end{aligned}$$

b. This can only hold if one of α'^2, α''^2 is even and the other odd. Since $(\pm 1)^2$ is the only odd integer square,

$$\Leftrightarrow \begin{cases} \alpha'^2 = 1 \wedge n\alpha''^2 = 0 \\ \alpha'^2 = 0 \wedge n\alpha''^2 = 1 \end{cases} \quad \Leftrightarrow \begin{cases} \alpha' = \pm 1 \wedge \alpha'' = 0 \\ \alpha' = 0 \wedge \alpha'' = \pm 1 \wedge n = 1 \end{cases}$$

c. $\mathbb{Z}\left[\sqrt{n}\right]$ is an integral domain because it has no divisors of zero because it has a multiplicative norm, so by Exercise 13 and (b.) every nonzero nonunit has a factorization into irreducibles.

18. Let $\alpha, \beta \in \mathbb{Z}\left[\sqrt{-2}\right] : \alpha = \alpha' + i\alpha'', \beta = \beta' + i\beta'', \beta \neq 0$ and let $q = \alpha/\beta = q' + iq'', \quad q', q'' \in \mathbb{Q}$, and let $\sigma = \sigma' + i\sigma'', \quad \sigma', \sigma'' \in \mathbb{Z}$ as close as possible to q so that $\left|\sigma' - q'\right|, \left|\sigma'' - q''\right| \leq \frac{1}{2}$. Then $N(q - \sigma) = N\left(\left(q' + iq''\right) - \left(\sigma' + i\sigma''\right)\right) = N\left(\left(q' - \sigma'\right) + \left(q'' - \sigma''\right)i\right) \leq \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^2 = \frac{1}{4} + \frac{2}{4} = \frac{3}{4}$ and $\nu\rho = N\rho = N(\alpha - \beta\sigma) = N\left(\beta \cdot \left(\alpha/\beta - \sigma\right)\right) = N\beta \cdot N(q - \sigma) \leq N\beta \cdot \frac{3}{4} < N\beta = \nu\beta$, so $\mathbb{Z}\left[\sqrt{n}\right]$ is a Euclidean domain.

Similarly for $\mathbb{Z}\left[\sqrt{n}\right]$, $N(q - \sigma) = \ldots \leq n \cdot \left(\frac{1}{2}\right)^2 = \frac{1}{4}n$ and $\nu\rho = \ldots \leq N\beta \cdot \frac{1}{4}n \overset{n=2,3}{<} N\beta = \nu\beta$ so $\mathbb{Z}\left[\sqrt{2}\right], \mathbb{Z}\left[\sqrt{3}\right]$ are Euclidean domains.

§8.1 Introduction to Extension Fields

♥ So "extension field" is just "superfield."

1. $x = 1 + \sqrt{2} \quad \Rightarrow x - 1 = \sqrt{2} \quad \Rightarrow (x - 1)^2 = x^2 - 2x + 1 = 2 \quad \Rightarrow x^2 - 2x - 1 = 0$.

2. $x = \sqrt{2} + \sqrt{3} \quad \Rightarrow x^2 = \left(\sqrt{2} + \sqrt{3}\right)^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$

$\Rightarrow x - 5 = 2\sqrt{6} \quad \Rightarrow (x - 5)^2 = x^2 - 10x + 25 = 4 \cdot 6 = 24 \quad \Rightarrow x^2 - 10x + 1 = 0$

3. $x = 1 + i \quad \Rightarrow x - 1 = i \quad \Rightarrow \left(x - 1\right)^2 = x^2 - 2x + 1 = -1 \quad \Rightarrow x^2 - 2x + 2 = 0$.

4. $x = \sqrt{1 + \sqrt[3]{2}} \quad \Rightarrow x^2 = 1 + \sqrt[3]{2} \quad \Rightarrow \left(x^2 - 1\right)^3 = \left(x^2 + 1\right)\left(x^4 - 2x^2 + 1\right) = x^6 - 2x^4 + x^2 + x^4 - 2x^2 + 1$

$= x^6 - x^4 - x^2 + 1 = 2 \quad \Rightarrow x^6 - x^4 - x^2 - 1 = 0$

5. $x = \sqrt{\sqrt[3]{2} - i} \quad \Rightarrow x^2 = \sqrt[3]{2} - i \quad \Rightarrow x^2 + i = \sqrt[3]{2}$

$\left(x^2 + i\right)^3 = \left(x^2 + i\right)\left(x^2 + i\right)^2 = \left(x^2 + i\right)\left(x^4 + 2x^2 i - 1\right) = \left(x^6 + 2x^4 i - x^2 + x^4 i - 2x^2 - i\right) = 2$

$\left(x^6 - 3x^2 - 2\right) = \left(-3x^4 + 1\right)i$

$\left(x^6 - 3x^2 - 2\right)^2 = -\left(-3x^4 + 1\right)^2 \quad \Rightarrow \left(x^6 - 3x^2 - 2\right)^2 + \left(-3x^4 + 1\right)^2 = 0$

$x^{12} - 3x^8 - 2x^6 - 3x^8 + 9x^4 + 6x^2 - 2x^6 + 6x^2 + 4 + 9x^8 - 6x^4 + 1 = 0$

$x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5 = 0$

6. $x = \sqrt{3 - \sqrt{6}} \quad \Rightarrow x^2 = 3 - \sqrt{6} \quad \Rightarrow x^2 - 3 = -\sqrt{6}$

$\Rightarrow \left(x^2 - 3\right)^2 = x^4 - 6x^2 + 9 = 6 \quad \Rightarrow x^4 - 6x^2 + 3 = 0$

$\operatorname{irr}\left(\sqrt{3 - \sqrt{6}}, \mathbb{Q}\right) = x^4 - 6x^2 + 3; \quad \deg\left(\sqrt{3 - \sqrt{6}}, \mathbb{Q}\right) = 4$

7. $x = \sqrt{\tfrac{1}{3} + \sqrt{7}} \quad \Rightarrow x^2 = \tfrac{1}{3} + \sqrt{7} \quad \Rightarrow x^2 - \tfrac{1}{3} = \sqrt{7} \quad \Rightarrow \left(x^2 - \tfrac{1}{3}\right)^2 = x^4 - \tfrac{2}{3}x^2 + \tfrac{1}{9} = 7$

$\Rightarrow \operatorname{irr}\left(\sqrt{\tfrac{1}{3} + \sqrt{7}}, \mathbb{Q}\right) = x^4 - \tfrac{2}{3}x^2 - 6\tfrac{8}{9}; \quad \deg\left(\sqrt{\tfrac{1}{3} + \sqrt{7}}, \mathbb{Q}\right) = 4$

8. $x = \sqrt{2} + i \quad \Rightarrow x - i = \sqrt{2} \quad \Rightarrow \left(x - i\right)^2 = x^2 - 2ix - 1 = 2 \quad \Rightarrow x^2 - 3 = 2ix \quad \Rightarrow \left(x^2 - 3\right)^2 = x^4 - 6x^2 + 9 = -4x^2$

$\Rightarrow \operatorname{irr}\left(\sqrt{2} + i, \mathbb{Q}\right) = x^4 - 2x^2 + 9; \quad \deg\left(\sqrt{2} + i, \mathbb{Q}\right) = 4$

9. $x = i \quad \Rightarrow x^2 = -1 \quad \Rightarrow x^2 + 1 = 0$; algebraic with degree 2.

10. $x = 1 + i \quad \Rightarrow x - 1 = i \quad \Rightarrow \left(x - 1\right)^2 = x^2 - 2x + 1 = -1 \quad \Rightarrow x^2 - 2x + 2 = 0$; algebraic with degree 2.

11. $x = \sqrt{\pi}$; transcendental.

12. $x = \sqrt{\pi} \quad \Rightarrow x^2 = \pi \quad \Rightarrow x^2 - \pi = 0$; algebraic with degree 2.

13. idem.

14. $x = \pi^2$; transcendental.

15. $x = \pi^2 \quad \Rightarrow x - \pi^2 = 0$; algebraic with degree 1.

16. $x = \pi^2 \quad \Rightarrow x^3 = \pi^6$; algebraic with degree 3.

17. $\dfrac{x^2 + x + 1}{x - \alpha} = x + \left(\alpha + 1\right) \quad \Rightarrow \left(x^2 + x + 1\right) = \left(x - \alpha\right)\left(x + \alpha + 1\right)$.

18. a. Since the polynomial has no zero for any element of $\mathbb{Z}_3$, it is irreducible by Theorem 5.6.10.

α	$x^2 + 1$
0	1
1	2
2	2

b.

$+$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	2α
2	2	0	1	$2+\alpha$	$2+2\alpha$	α	2α	$1+\alpha$	$1+2\alpha$
α	α	$1+\alpha$	$2+\alpha$	2α	0	$1+2\alpha$	1	$2+2\alpha$	2
2α	2α	$1+2\alpha$	$2+2\alpha$	0	α	1	$1+\alpha$	2	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	1	$2+2\alpha$	2	2α	0
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	2α	1	$1+\alpha$	2	$2+\alpha$	0	α
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2	2α	0	$1+2\alpha$	1
$2+2\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	$2+\alpha$	0	α	1	$1+\alpha$

$\cdot$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	0	α	2α	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
2α	0	2α	α	1	2	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	$2+\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	2α	2	1	α
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	2	α	2α	1
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	1	2α	α	2
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	α	1	2	2α

where $\alpha+1=0 \Rightarrow \alpha^2=-1=2$.

19. "of some nonzero polynomial" in $F[x]$.

20. "nonzero"

21. are having "the coefficient of the highest-degree term" equal to 1.

22. Correct?

23. a. true (there is no polynomial over $\mathbb{Q}$ having π as a root)

    b. true

    c. true ($\forall f \in F : x-f \in F[x]$ has f as a root)

    d. true ($\mathbb{R} \supset \mathbb{Q}$)

    e. false ($\mathbb{Q} \not\supset \mathbb{Z}_2$ because addition on $\mathbb{Z}_2$ is not the one induced from $\mathbb{Q}$)

    f. true (Definition 14)

    g. false ($x^2-2 \in \mathbb{Q}[x]$ has degree 2 but $x-\sqrt{2} \in \mathbb{R}[x]$ has degree 1)

    h. true (Kronecker's Theorem)

    i. false ($\mathbb{R} \times \mathbb{Z}_2 \supset \mathbb{R}$ is an extension field but x^2+1 has no zero in it)

    j. true (as in the discussion after Example 19)

24. a. In $F=\left\langle 1,\pi^3 \right\rangle$, $\operatorname{irr}(\pi,F)=x^3-\pi^3$ with degree 3.

    b. In $E=\left\langle 1,e^{10} \right\rangle$, $\operatorname{irr}\left(e^2,E\right)=x^5-e^{10}$ with degree 5.

25. a. $\phi_{\mathbb{Z}_2}\left(x^3+x^2+1\right)=\{1\}$ has no zero in $\mathbb{Z}_2$, so no nonunit factors.

    b. $\dfrac{x^3+x^2+1}{x-\alpha}=x^2+(1+\alpha)x+\left(\alpha^2+\alpha\right)$, so $x^3+x^2+1=(x-\alpha)\left(x^2+(1+\alpha)x+\left(\alpha^2+\alpha\right)\right)$. To factorize the second factor, finding a zero by applying the elements of $\mathbb{Z}_2(\alpha)$: $0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1$. Eventually we find that $\phi_{\alpha^2}\left(x^2+(1+\alpha)x+\left(\alpha^2+\alpha\right)\right)=\left(\alpha^2\right)^2+(1+\alpha)\alpha^2+\alpha^2+\alpha \overset{*}{=} -\alpha^3+\alpha+\alpha^2+\alpha^3+\alpha^2+\alpha=0$, where

$\alpha^3+\alpha^2+1=0 \Rightarrow \alpha^3=-\left(\alpha^2+1\right)$; $\alpha^4=\alpha\cdot\alpha^3=-\alpha\cdot\left(\alpha^2+1\right)=-\alpha^3+\alpha$. Then $\dfrac{x^2+\left(1+\alpha\right)x+\left(\alpha^2+\alpha\right)}{x-\alpha^2}=x+\left(\alpha^2+\alpha+1\right)$, so $x^2+\left(1+\alpha\right)x+\left(\alpha+\alpha^2\right)=\left(x-\alpha\right)\left(x-\alpha^2\right)\left(x+\left(\alpha^2+\alpha+1\right)\right)$. ¿Note that the solution in the text has a minus sign in $x-\left(\alpha^2+\alpha+1\right)$?

26. $\deg\left(\alpha,\mathbb{Z}_2\right)=3 \quad \Rightarrow \alpha\in\mathbb{Z}_2\left(\alpha\right): x^3-\alpha=0$; $\mathbb{Z}_2\left(\alpha\right)=\left\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\right\}$. The table gives $\left\langle\mathbb{Z}_3\left(\alpha\right),+\right\rangle$:

0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

By the Fundamental Theorem of Finitely-Generated Commutative Groups, this has to be isomorphic to either $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_2$, or $\mathbb{Z}_8$. Since $\mathbb{Z}_4,\mathbb{Z}_8$ have elements of order 4 and 8, respectively, which $\mathbb{Z}_2\left(\alpha\right)$ does not, we must have $\mathbb{Z}_2\left(\alpha\right)\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\cong\left\{0,1\right\}\times\left\{0,\alpha\right\}\times\left\{0,\alpha^2\right\}$. $\left\langle\mathbb{Z}_2\left(\alpha\right)^*,\cdot\right\rangle$ has order 7 so it can only be isomorphic to $\mathbb{Z}_7$.

27. Because it is (Theorem 13) of minimal degree.

28.

29. By Theorem 18, $F\left(\alpha\right)=\left\{_{b_i\in F} \quad +_{i=0}^{n-1} b_i\alpha^i\right\}$ where each of the elements are unique, so $\left|F\left(\alpha\right)\right|=\left|F\right|^n=q^n$.

30. a. $x\left(x+1\right)\left(x+2\right)=x\left(x^2+3x+2\right)=x\left(x^2+2\right)=x^3+2x$ evaulates to zero for $x\in\left\{0,1,2\right\}=\mathbb{Z}_3$ so $x\left(x+1\right)\left(x+2\right)+1=x^3+2x+1$ evaluates to one over $\mathbb{Z}_3$ and is therefore irreducible.

b. By Exercise 29, $\left|\mathbb{Z}_3\left(\alpha\right)\right|=3^3=27$.

31. a. Since $1^2=1$ and $\left(p-1\right)^2=p^2-2p+1=_p 1$ there must be at least one element in $\mathbb{Z}_p$ that is not a square.

b. By (a.), there is an element $a\in\mathbb{Z}_p$ that is not a square, so x^2-a has no zero in $\mathbb{Z}_p$ so a is of degree 2 in $\mathbb{Z}_p\left(\alpha\right)$, and by Exercise 30b $\left|\mathbb{Z}_p\left(a\right)\right|=p^2$.

32. Because if $\beta\in F\left(\alpha\right)$ is algebraic then $\exists p\in F\left(\alpha\right):\phi_\beta p=0$ and then $\exists p'\in F\left(\alpha\right):\phi_\alpha p'=\phi_{\alpha+\beta-\alpha}p$ such that $\phi_\alpha p'=\phi_\beta p=0$, and α would be algebraic also. It is clear that p' is in fact polynomial also.

33. It is clear that $\left\{_{a,b,c\in\mathbb{Q}} \quad a+b\cdot\sqrt[3]{2}+c\cdot\left(\sqrt[3]{2}\right)^2\right\}\subset\mathbb{R}$ is the simple extension $\mathbb{Q}\left(\sqrt[3]{2}\right)$ described by Theorem 18 and a field, and that $\mathbb{Q}\left(\sqrt[3]{2}\right)\subset\mathbb{R}$.

34. i. Since $8=2^3$, we look for an irreducible polynomial of degree 3 in $\mathbb{Z}_2$: $x\cdot\left(x-1\right)\cdot x+1=x^3-x^2+1$. So $\mathbb{Z}_2\left(\alpha\right)\cong\dfrac{\mathbb{Z}_2\left[x\right]}{\left\langle x^3-x^2+1\right\rangle}$ and $\left|\mathbb{Z}_2\left(\alpha\right)\right|=2^3=8$ (Exercise 25).

ii. Since $16 = 2^4$, we look for an irreducible polynomial of degree 4 in $\mathbb{Z}_2$: $x \cdot (x-1) \cdot x^2 + 1 = x^4 - x^3 + 1$. So

$$\mathbb{Z}_2(\alpha) \cong \frac{\mathbb{Z}_2[x]}{\langle x^4 - x^3 + 1 \rangle} \text{ and } |\mathbb{Z}_2(\alpha)| = 2^4 = 16.$$

iii. Since $25 = 5^2$, we look for an irreducible polynomial of degree 5 in $\mathbb{Z}_5$. Since $\phi_{\mathbb{Z}_5}(x^2 + 3) = \{2, 3, 4\}$ that one is irreducible and $\mathbb{Z}_5(\alpha) \cong \dfrac{\mathbb{Z}_5[x]}{\langle x^2 + 3 \rangle}$ and $|\mathbb{Z}_5(\alpha)| = 5^2 = 25$ (Exercise 31b).

35. Since F is finite it is of prime characteristic and contains a prime subfield $\mathbb{Z}_p \subseteq F$ (Theorem 6.2.19). By Theorem 5.3.1, $\forall a \in \mathbb{Z}_p^* : a^{p-1} =_p 1 \quad \Rightarrow \phi_a(x^{p-1} - 1) = 0$ and algebraic over $\mathbb{Z}_p$.

36. By Exercise 35 every finite field can be considered an extension of its prime subfield. Then by Exercise 29, the order of the field is a prime power.

§8.2 Vector Spaces

♥ 1 So, dimensionality does not even enter into the definition of a vector space— the defining aspect is only scalar multiplication with a field. It's almost like a *G*-set (Definition 3.5.1) except *X* has to be an actual group and *G* a field. Note in particular that no relationship between *V* and *F* is implied.

♥ 4 This seems profound but is almost meaningless: any superfield can be regarded as a vector space in the same way that any field is a vector space.

1. $\{(0,1),(1,1)\}, \quad \{(1,0),(1,-1)\}, \quad \{(-1,0),(-1,-1)\}.$

2. Since

$$\begin{bmatrix}1 & 0 & 0\end{bmatrix} = \tfrac{1}{2}\left(\begin{bmatrix}1 & 1 & 0\end{bmatrix} + \begin{bmatrix}1 & 0 & 1\end{bmatrix} - \begin{bmatrix}0 & 1 & 1\end{bmatrix}\right)$$
$$\begin{bmatrix}0 & 1 & 0\end{bmatrix} = \tfrac{1}{2}\left(\begin{bmatrix}1 & 1 & 0\end{bmatrix} + \begin{bmatrix}0 & 1 & 1\end{bmatrix} - \begin{bmatrix}1 & 0 & 1\end{bmatrix}\right)$$
$$\begin{bmatrix}0 & 0 & 1\end{bmatrix} = \tfrac{1}{2}\left(\begin{bmatrix}0 & 1 & 1\end{bmatrix} + \begin{bmatrix}1 & 0 & 1\end{bmatrix} - \begin{bmatrix}1 & 1 & 0\end{bmatrix}\right)$$

and by Lemma 16, this set of vectors obviously spans $\mathbb{R}^3$. Since $\dim \mathbb{R}^3 = 3$, by Theorem 17 this is a basis.

3.
$$\begin{cases} -1x + 1y + 2z = 0 \\ 2z - 3y + 1z = 0 \\ 10x - 14y = 0 \end{cases} \Rightarrow \begin{cases} -\frac{4}{10}y + 2z = 0 \\ -\frac{1}{5}y + 1z = 0 \\ 10x - 14y = 0 \end{cases} \Rightarrow \begin{cases} -y + 5z = 0 \\ 5x - 7y = 0 \end{cases}$$

so not linearly independent by Definition 10, and hence not a basis.

4. $\{1, \sqrt{2}\}$.

5. $\{1\}$.

6. $\{2^{0/3}, 2^{1/3}, 2^{2/3}\}$.

7. $\{1, i\}$.

8. $\{1, i\}$

9. $\{2^{0/4}, 2^{1/4}, 2^{2/4}, 2^{3/4}\}$.

10. The same polynomial of Example 1.19 has a zero for $1 + \alpha$:

$$\phi_{1+\alpha}(x^2 + x + 1) = (1+\alpha)^2 + (1+\alpha) + 1 = 1 + \alpha^2 + \alpha = 1 + \alpha + 1 + \alpha = 0.$$

11. Delete “uniquely.”

12. Correct.

13. Correct.

14. “independent.”

15. a. true ($\forall \alpha, \beta \in V : \alpha + \beta \in V$)
b. false ($\forall a, b \in F : a + b \in F$)
c. true ($\forall a, b \in F : a \cdot b \in F$)
d. true ($\forall a \in F, \alpha \in V : a\alpha \in V$)
e. false ($F\left[x\right]$ has an infinite basis, Example 7)
f. false (Definition 15)
g. false (wouldn't be linearly independent)
h. true (Theorem 23)
i. true (idem)
j. true (discussion before Lemma 16)

16. a. A subspace of a vector space V over F is a vector space of a subgroup of V over F with the induced operations.
b. We have to show that the intersection is closed. Let U, V be subspaces over F:
$\forall \alpha, \beta \in U \cap V : \alpha + \beta \in U, \alpha + \beta \in V \Rightarrow \alpha + \beta \in U \cap V$,
$\forall \alpha \in U \cap V, a \in F : a\alpha \in U, a\alpha \in V \Rightarrow a\alpha \in U \cap V$.

17.

18.

19.

20.

21. If every vector in V can be generated by the β_i then they certainly span at least V. If the zero vector is the sum of none of the β_i, and the zero vector can be expressed only uniquely as a linear combination of β_i, then they are linearly independent. So β_i are a basis. Conversely, if β_i are a basis then they span V. Each vector is a unique linear combincation of the β_i, otherwise the difference between two expressions of the same vector would give a linear combination of the zero vector and β_i would not be linearly independent.

22. a. Considering the vector space F^m over F, we have $\forall i : +_j^n a_{ij} x_j = b_i \quad \Leftrightarrow \quad +_j \, x_j \mathbf{a}_j = \mathbf{b}$, where $\mathbf{a}_j = \left(a_{0j} \ldots a_{m-1,j}\right)$, $\mathbf{b} = \left(b_0 \ldots b_{m-1}\right) \in F^m$. The system has a solution iff $\mathbf{b}$ is in the span of $\left\{_j \, \mathbf{a}_j\right\}$.
b. By the Exercise, every $\beta \in F^m$ can be expressed uniquely as a linear combination of the basis $\left\{_j \, \mathbf{a}_j\right\}$.

23. They are naturally isomorphic by their ‘coefficients’. Let $\left\{_{i=0}^{n-1} \, \mathbf{v}_i\right\}$ and $\left\{_{i=0}^{n-1} \, \mathbf{f}_i\right\}$ be bases for V and F^n, respectively.
Then $\psi : V \to F^n : \mathbf{x} = +_i x_i \mathbf{v}_i \mapsto +_i x_i \mathbf{f}_i$ is an isomorphism: $\forall \mathbf{x} = +_i x_i \mathbf{v}_i, \mathbf{y} = +_i y_i \mathbf{v}_i \in V$:

$$\psi\left(\mathbf{x} + \mathbf{y}\right) = \psi\left(+_i x_i \mathbf{v}_i + +_i y_i \mathbf{v}_i\right) = \psi\left(+_i \left(x_i + y_i\right) \mathbf{v}_i\right)$$
$$= +_i \left(x_i + y_i\right) \mathbf{f}_i = +_i x_i \mathbf{f}_i + +_i y_i \mathbf{f}_i = \psi\left(+_i x_i \mathbf{v}_i\right) + \psi\left(+_i x_i \mathbf{v}_i\right) = \psi\mathbf{x} + \psi\mathbf{y}$$

and $\forall a \in F, \mathbf{x} = +_i x_i \mathbf{v}_i \in V$:

$$\psi\left(a\mathbf{x}\right) = \psi\left(a \cdot +_i x_i \mathbf{v}_i\right) = \psi\left(+_i a \cdot \left(x_i \mathbf{v}_i\right)\right) = \psi\left(+_i \left(a x_i\right) \mathbf{v}_i\right)$$
$$= +_i \left(a x_i\right) \mathbf{f}_i = +_i a \cdot \left(x_i \mathbf{f}_i\right) = a \cdot +_i x_i \mathbf{f}_i = a \cdot \psi\left(+_i x_i \mathbf{v}_i\right) = a \cdot \psi\mathbf{x}$$

24. a. $\forall \mathbf{v} = +_i v_i \beta_i : \phi\mathbf{v} = \phi\left(+_i v_i \beta_i\right) = +_i \phi\left(v_i \beta_i\right) = +_i v_i \phi\beta_i$.
b. Since by (a.) a linear transformation is completely determined by its action on the basis vectors, the action required for the basis vectors specified here suffices.

25. a. homomorphism.
b. The nullspace of ϕ is the set of vectors $v \in V : \phi v = 0$. To show that $\operatorname{Ker}\phi \subseteq V$ is a subspace we have to show that it is closed under the induced operations from V:
$\forall v, w \in \operatorname{Ker}\phi : \phi\left(v + w\right) = \phi v + \phi w = 0 + 0 = 0 \quad \Rightarrow v + w \in \operatorname{Ker}\phi$.
c. When it is a homomorphism (linear transformation) with $\operatorname{Ker}\phi = E$.

26. The quotient space V/S over F is the vector space in the group of cosets of S in V over F, with scalar multiplication by representatives in V. The coset group exists by Corollary 3.2.5 and is clearly commutative. Show that the five

conditions of a vector space hold: $\forall a,b \in F : \alpha + S, \beta + S \in V/S$:

(1) $a(\alpha + S) = a\alpha + S \in V/S$;

(2) $a \cdot (b \cdot (\alpha + S)) = a \cdot (b\alpha + S) = ab\alpha + S = ab(\alpha + S)$;

(3) $(a+b)(\alpha + S) = (a+b)\alpha + S = (a\alpha + b\alpha) + S = ((a\alpha) + S) + ((b\alpha) + S) = a \cdot (\alpha + S) + b \cdot (\alpha + S)$;

(4) $a((\alpha + S) + (\beta + S)) = a((\alpha + \beta) + S) = a(\alpha + \beta) + S = (a\alpha + a\beta) + S = (a\alpha + S) + (a\beta + s)$;

(5) $1(\alpha + S) = 1\alpha + S = \alpha + S$.

27. a. We know that ϕ is a homomorphiosm so that operations under ϕ coincide with the ones induced from V'. We need to show that $\phi V \subseteq V'$ is closed:

$\forall \alpha', \beta' \in \phi V : \exists \alpha, \beta \in V : \phi\alpha = \alpha', \phi\beta = \beta' \Rightarrow \phi(\alpha + \beta) = \phi\alpha + \phi\beta = \alpha' + \beta' \in \phi V$.

b. Let $\{_i\ \alpha_i\}$ be a basis for $\operatorname{Ker}\phi \subseteq V$. To this basis can be adjoined $\dim V - \dim \operatorname{Ker}\phi$ vectors to form a basis for V. Since $\psi : V/\operatorname{Ker}\phi \to \phi V$ is an isomorphism, we have $\dim \phi V = \dim V - \dim \operatorname{Ker}\phi$.

§8.3 Algebraic Extensions

So we have two ways of determining the degree of an extension: by the order of the basis, and by the degree of the irreducible polynomial.

1. $\deg\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$, so by Theorem 2.23 , $\{2^{0/2}, 2^{1/2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$.

2. $\{2^{0/2}, 2^{1/2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. It is 'clear' that $\sqrt{3}$ cannot be axpressed as a linear combination of this basis, so $\{3^{0/2}, 3^{1/2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. By Theorem 4, $\{1, 3^{1/2}, 2^{1/2}, 6^{1/2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ and $\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right] = 4$.

3. $\sqrt{18} = 3\sqrt{2} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so from Exercise 2, $\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}) : \mathbb{Q}\right] = 4$ and $\{1, 3^{1/2}, 2^{1/2}, 6^{1/2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$ over $\mathbb{Q}$.

4. $\{2^{0/3}, 2^{1/3}, 2^{2/3}\}$ is a basis for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Since $\deg(\sqrt{3}, \mathbb{Q}) = 2$ does not divide $\deg(\sqrt[3]{2}) = 3$, $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$ and by Theorem 4, $\{1, 2^{1/3}, 2^{2/3}, 3^{1/2}, 2^{1/3} \cdot 3^{1/2}, 2^{2/3} \cdot 3^{1/2}\}$ spans $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ over $\mathbb{Q}$. Since this set is linearly independent, it forms a basis, and $\left[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}\right] = 4$.

5. $\{2^{0/2}, 2^{1/2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. $\deg(\sqrt[3]{2}, \mathbb{Q}) = 3$ does not divide $\deg(\sqrt{2}, \mathbb{Q}) = 2$, so $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. So $\{2^{0/3}, 2^{1/3}, 2^{2/3}\}$ is a basis for $\mathbb{Q}(2^{1/3}, 2^{1/2})$ over $\mathbb{Q}(2^{1/2})$ and by Theorem 4, $\{2^{0/6}, 2^{2/6}, 2^{4/6}, 2^{3/6}, 2^{5/6}, 2^{7/6}\}$ is a basis for $\mathbb{Q}(2^{1/3}, 2^{1/2})$ over $\mathbb{Q}$. Try to simplify the basis. $2^{7/6} = 2 \cdot 2^{1/6}$, so $2^{1/6} \in \mathbb{Q}(2^{1/3}, 2^{1/2})$ and $\mathbb{Q}(2^{1/3}, 2^{1/2}) \supseteq \mathbb{Q}(2^{1/6})$. $\phi_{1/6}(x^6 - 2) = 0$ is an Eisenstein polynomial for $p = 2$ and irreducible over $\mathbb{Q}$, so $\mathbb{Q}(2^{1/6}) \supset \mathbb{Q}$, and $\mathbb{Q}(2^{1/3}, 2^{1/2}) \supseteq \mathbb{Q}(2^{1/6}) \supset \mathbb{Q}$. Then

$$\left[\mathbb{Q}(2^{1/3}, 2^{1/2}) : \mathbb{Q}\right] = \left[\mathbb{Q}(2^{1/3}, 2^{1/2}) : \mathbb{Q}(2^{1/6})\right] \cdot \left[\mathbb{Q}(2^{1/6}) : \mathbb{Q}\right]$$

$$6 = \left[\mathbb{Q}(2^{1/3}, 2^{1/2}) : \mathbb{Q}(2^{1/6})\right] \cdot 6$$

and $\left[\mathbb{Q}(2^{1/3}, 2^{1/2}) : \mathbb{Q}(2^{1/6})\right] = 1$, so by the discussion after Definition 2, $\left[\mathbb{Q}(2^{1/3}, 2^{1/2}) : \mathbb{Q}(2^{1/6})\right]$. So

$\left[\mathbb{Q}\left(2^{1/3},2^{1/2}\right),\mathbb{Q}\right]=6$ and $\left\{_{0\le i<6}\;2^{i/6}\right\}$ is a basis.

6. $x=\sqrt{2}+\sqrt{3}\overset{\text{Exercise 8.1}}{\Rightarrow}x^2-10x+1=0$. $\left\{1,\sqrt{2}+\sqrt{3}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$, and $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\right]=2$.

7. $\left\{1,\sqrt{6}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{6}\right)$, and $\left[\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right]=2$.

8. Analogous to Exercise 4, $\left\{_{0\le i<2,0\le j<3}\;2^{i/2}\cdot 5^{j/3}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2},\sqrt[3]{5}\right)$, and $\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{5}\right):\mathbb{Q}\right]=6$.

9. $\sqrt[3]{24}=2\sqrt[3]{6}$, so $\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}\right)=\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{6}\right)$. $\sqrt[3]{6}=\sqrt[3]{2}\cdot\sqrt[3]{3}$, so $\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{6}\right)=\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{3}\right)$ (¿why?). Then $\left\{_{0\le i<3,0\le j<3}\;2^{i/3}\cdot 3^{j/3}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}\right)$ over $\mathbb{Q}$, and $\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{6},\sqrt[3]{24}\right):\mathbb{Q}\right]=9$.

10. $\mathbb{Q}\left(\sqrt{2},\sqrt{6}\right)=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$, so $\left\{1,\sqrt{2}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2},\sqrt{6}\right)$ over $\mathbb{Q}\left(\sqrt{3}\right)$ and $\left[\mathbb{Q}\left(\sqrt{2},\sqrt{6}\right):\mathbb{Q}\right]=2$.

11. $\sqrt{2}+\sqrt{3}\notin\mathbb{Q}\left(\sqrt{3}\right)$, so $\sqrt{2}\notin\mathbb{Q}\left(\sqrt{3}\right)$ and $\left\{2^{0/2},2^{1/2}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ over $\mathbb{Q}$, $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\right]=2$.

12. By Theorem 4,

$$\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]=\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\left(\sqrt{3}\right)\right]$$

$$2=\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)\right]\cdot 2$$

so $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)\right]=1$ (?!?)

13. $\sqrt{2}\notin\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$ but $\sqrt{6}+\sqrt{10}\in\mathbb{Q}\left(\sqrt{3}+\sqrt{5},\sqrt{2}\right)$, so $\left\{2^{0/2},2^{1/2}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2},\sqrt{6}+\sqrt{10}\right)$ over $\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$.

14. “is a field *E* where each element of *E* is”

15. “to a basis for *F*”

16. Correct.

17. “nonconstant polynomial over *F*”

18. $\overline{\mathbb{Q}}_{\mathbb{R}}$ (the algebraic numbers) are real elements such as $\sqrt{2}$ that have polynomials in $\mathbb{Q}[x]$ such as x^2-2 with those elements as zeroes. However, $\overline{\mathbb{Q}}_{\mathbb{R}}[x]$ has polynomials such as x^2+1 with imaginary roots that are not in $\mathbb{Q}_{\mathbb{R}}$.

19. a. true (Theorem 3)

b. false (the extension of $\mathbb{Q}$ containing all powers of π, $\mathbb{Q}[\pi]$, is algebraic and infinite)

c. true (Theorem 4)

d. false ($x^2+1\in\mathbb{R}[x]$ has no zero in $\mathbb{R}$)

e. false ($x^2-2\in\mathbb{Q}[x]$, but the root $\sqrt{2}\notin\mathbb{Q}$ so $\overline{\mathbb{Q}}_{\mathbb{R}}\supset\mathbb{Q}$)

f. true (the only elements of $\mathbb{Q}(x)$ that are algebraic in $\mathbb{C}$ are $\mathbb{C}$ itself; for example, $x-1$ has no root in $\mathbb{C}[y]$)

g. false (the polynomial $(x+1)y+x\in\mathbb{C}(x)[y]$ does not have a root y)

h. false (Theorem 17)

i.

j. false ($\mathbb{C}$ is an algebraically closed extension of $\mathbb{Q}$, but $\pi\in\mathbb{C}$ shows that $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$)

20. Since $a+bi\notin\mathbb{R}$, $\left\{1,a+bi\right\}$ is a basis for $\mathbb{R}(a+bi)$ over $\mathbb{R}$ and $\left[\mathbb{R}(a+bi):\mathbb{R}\right]=2$. Similarly, $\left[\mathbb{C}:\mathbb{R}\right]=2$, so

$$\left[\mathbb{C}:\mathbb{R}\right]=\left[\mathbb{C}:\mathbb{R}(a+bi)\right]\cdot\left[\mathbb{R}(a+bi):\mathbb{R}\right]\quad\Rightarrow\left[\mathbb{C}:\mathbb{R}(a+bi)\right]=\frac{\left[\mathbb{C}:\mathbb{R}\right]}{\left[\mathbb{R}:\mathbb{R}(a+bi)\right]}=\frac{2}{2}=1.$$ So $\mathbb{C}=\mathbb{R}(a+bi)$.

21. Since $E \supseteq F$ is a finite extension and $\left[E:F\right]$ is prime, E is a simple extension of F, $\exists \alpha \in E \setminus F : E = F\left(\alpha\right)$. Consider $F\left(\alpha\right)$ for any $\alpha \in E \setminus F$. Then $\left\{1, \alpha\right\}$ is a basis for $F\left(\alpha\right)$ over F and $\left[E:F\right] = \left[E:F\left(\alpha\right)\right] \cdot \left[F\left(\alpha\right):F\right] \quad \Rightarrow \left[E:F\left(\alpha\right)\right] = \dfrac{\left[E:F\right]}{\left[F\left(\alpha\right):F\right]} = \tfrac{1}{2}\left[E:F\right]$ which is impossible because $\left[E:F\right]$ is prime, so $\left[E:F\right] = 2$ and $\left[E:F\left(\alpha\right)\right] = 1$ so $E = F\left(\alpha\right)$ is simple.

22. $x^2 - 3$ has roots $\pm\sqrt{3} \notin \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{Q}$.

23. Every root increases the degree of the field by a factor of 2, so $\left[\mathbb{Q}\left({}_{i}^{n}\sqrt{p_i}\right) : \mathbb{Q}\right] = 2^n$. Since a zero of $x^{14} - 3x^2 + 12$ has degree $14 = 2 \cdot 7$, which does not divide 2^n, there is no element of $\mathbb{Q}\left({}_{i}^{n}\sqrt{p_i}\right)$ that can be such a zero.

24. Since E is a finite extension, by Theorem 11 $\exists \alpha_i : E = F\left({}_i\ \alpha_i\right)$. Let $g, h \in D \subseteq E;\ g, h \neq 0$, so $g = +_i\ g_i \alpha_i, \quad h = +_i\ h_i \alpha_i$. Since $g, h \neq 0$ and the extension is finite, there are maximal $\exists j, k : g_j, h_k \neq 0$, so $g \cdot h = +_{i,j}\ g_i h_j \alpha^{i+j}$.

25. Since $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{7}\right)$, $\left\{1, \sqrt{3}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right)$ over $\mathbb{Q}\left(\sqrt{7}\right)$, so $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{7}\right)\right] = 2$. Now consider:

$$x = \sqrt{3} + \sqrt{7} \quad \Rightarrow x - \sqrt{3} = \sqrt{7} \quad \Rightarrow \left(x - \sqrt{3}\right)^2 = 7 \quad \Rightarrow x^2 - 2\sqrt{3} + 3 = 7 \quad \Rightarrow x^2 - 4 = 2\sqrt{3}$$

$$\Rightarrow \left(x^2 - 4\right)^2 = 4 \cdot 3 = 12 \quad \Rightarrow x^4 - 8x^2 + 16 = 12 \quad \Rightarrow x^4 - 8x^2 + 28 = 0$$

so $\deg\left(\sqrt{3} + \sqrt{7}, \mathbb{Q}\right) = 4$ and $\left[\mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right) : \mathbb{Q}\right] = 4$, so

$$\begin{aligned} \left[\mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right) : \mathbb{Q}\right] &= \left[\mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{7}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] \\ 4 &= \left[\mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{7}\right)\right] \cdot 2 \\ 2 &= \left[\mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{7}\right)\right] \end{aligned}$$

Then:

$$\begin{aligned} \left[\mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{7}\right)\right] &= \left[\mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{7}\right)\right] \\ 2 &= \left[\mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right)\right] \cdot 2 \\ 1 &= \left[\mathbb{Q}\left(\sqrt{3}, \sqrt{7}\right) : \mathbb{Q}\left(\sqrt{3} + \sqrt{7}\right)\right] \end{aligned}$$

26.

27. A zero β of an irreducible p is of degree $\deg\left(\beta, F\right) = \deg p$ and $\deg\left(\beta, F\right) = \left[F\left(\beta\right) : F\right]$. But $E \supseteq F\left(\beta\right) \supseteq F$, and so $\left[F\left(\beta\right) : F\right] = \deg p$ would not divide $\left[E:F\right]$, which is impossible by Theorem 14.

28. If α is of degree 1, $\alpha, \alpha^2 \in F$ and $F\left(\alpha\right) = F\left(\alpha^2\right) = F$. Suppose n is of at least degree 3. By Theorem 2.23, $F\left(\alpha\right)$ has basis $\left\{{}_{i=0}^{n-1}\ \alpha^i\right\}$, where $n = \deg\left(\alpha, F\right)$. Since 2 is relatively prime to n, 2 generates $\mathbb{Z}_n$ by Corollary 1.5.18 and $\left\{{}_{i=0}^{n-1}\left(\alpha^2\right)^i\right\} = \left\{{}_{i=0}^{n-1}\ \alpha^i\right\}$ and $F\left(\alpha^2\right) = F\left(\alpha\right)$.