Concrete Abstract Algebra

Exercise Solutions

Rasmus Villemoes

Department of Mathematical Sciences
University of Aarhus
2004

Concrete Abstract Algebra — Exercise Solutions
Rasmus Villemoes <burner@imf.au.dk>
Version 1.0, 2004
Typeset by the author using LaTeX and METAPOST.

Contents

Preface

This document contains solutions to the exercises in the undergraduate algebra textbook “Concrete Abstract Algebra” by Niels Lauritzen (Cambridge University Press, October 2003). The solutions are only intended as a guide and should not be taken as the only correct answers. There may well be several different approaches leading to the same results.

The notes are meant as a help to teachers as well as their students. It is entirely up to the lecturer to decide whether this document is made available to the students; both possibilities have its advantages and disadvantages.

If you find an error, be it mathematical, typographical, grammatical or other, if you find a simpler solution to an exercise, or if you have comments of any kind, I would love to hear from you. My email address is burner@imf.au.dk.

The latest version of this document is available through Cambridge University Press.

Have fun!

D03, 25th March 2004

BSc student Rasmus Villemoes
Department of Mathematical Sciences
University of Aarhus, Denmark
burner@imf.au.dk
http://home.imf.au.dk/burner/

Chapter 1

Ex. 1.1 Assume the subset $S \subseteq \mathbb{Z}$ has two "first elements", denote them x and y. Then by definition we have that for every $s \in S$, $x \leq s$ and $y \leq s$; these inequalities also hold in the special cases $s = y$ and $s = x$. Thus $x \leq y$ and $y \leq x$, which by definition means $y - x \in \mathbb{N}$ and $x - y = -(y - x) \in \mathbb{N}$. But the only element $z \in \mathbb{N}$ for which also $-z \in \mathbb{N}$ is 0; so we must in fact have $y - x = 0$, implying $x = y$.

Ex. 1.2 Let $x, d \in \mathbb{Z}$, $d > 0$. Let $M = \{x - qd \mid q \in \mathbb{Z}\}$. If $x \in \mathbb{N}$ then $x \in M \cap \mathbb{N}$ (with $q = 0$), which is therefore not empty. If $x < 0$, let $q = x$. Then $x - xd = x(1 - d) \in M$, and since $1 - d \leq 0$ we have $x(1 - d) \in \mathbb{N}$.

Ex. 1.3 Let $a, b, N \in \mathbb{Z}$, $N > 0$. Let $[\,\cdot\,]$ denote remainder by division with N. From Proposition 1.3.2(i) we have

$$a \equiv [a] \pmod{N} \tag{1.1}$$
$$b \equiv [b] \pmod{N} \tag{1.2}$$

and then from Proposition 1.3.4(ii) we have

$$ab \equiv [a][b] \pmod{N}. \tag{1.3}$$

Finally from Proposition 1.3.2(ii) we have

$$[ab] = \big[[a][b]\big]$$

Ex. 1.4 Everywhere in the following the notation $[\,\cdot\,]$ denotes the remainder by division with 341. The representation of 340 in the binary number system is 101010100. The repeated squaring algorithm requires us to build the following table. Note that $2^{2^n} = 2^{2^{n-1}+2^{n-1}} = 2^{2^{n-1}}2^{2^{n-1}} = (2^{2^{n-1}})^2$.

$$
\begin{aligned}
[2] &= 2\\
\left[2^2\right] &= 4\\
\left[2^{2^2}\right] &= \left[(2^2)^2\right] = \left[[2^2]^2\right] = \left[4^2\right] = 16\\
\left[2^{2^3}\right] &= \left[(2^{2^2})^2\right] = \left[[2^{2^2}]^2\right] = [256] = 256\\
\left[2^{2^4}\right] &= \left[[2^{2^3}]^2\right] = \left[256^2\right] = 64\\
\left[2^{2^5}\right] &= \left[[2^{2^4}]^2\right] = \left[64^2\right] = 4\\
\left[2^{2^6}\right] &= \left[[2^{2^5}]^2\right] = \left[4^2\right] = 16\\
\left[2^{2^7}\right] &= \left[[2^{2^6}]^2\right] = \left[16^2\right] = 256\\
\left[2^{2^8}\right] &= \left[[2^{2^7}]^2\right] = \left[256^2\right] = 64
\end{aligned}
$$

To find $[2^{340}]$ one does a few simple calculations:

$$
\begin{aligned}
\left[2^{340}\right] &= \left[2^{256+64+16+4}\right]\\
&= \left[[2^{256}][2^{64}][2^{16}][2^4]\right]\\
&= \left[[2^{2^8}][2^{2^6}][2^{2^4}][2^{2^2}]\right]\\
&= [64 \cdot 16 \cdot 64 \cdot 16]\\
&= \left[[64^2][16^2]\right]\\
&= [4 \cdot 256]\\
&= [1024]\\
&= 1,
\end{aligned}
$$

which was to be shown.

One may also to observe that $2^{340} = \left(2^{10}\right)^{34}$, and use the product rule:

$$
\begin{aligned}
\left[2^{340}\right] &= \left[\left(2^{10}\right)^{34}\right]\\
&= [1024]^{34}\\
&= 1^{34}\\
&= 1
\end{aligned}
$$

Ex. 1.5 (i) $2 + 2 \cdot 3 + 1 \cdot 3^2$ is a 3-adic expansion of 17.

(ii) Let $x \in \mathbb{N}$ be a positive number. Define $r = \max\{s \in \mathbb{N} \mid \tau^s \leq x\}$. Letting $d = \tau^r$, from Theorem 1.2.1 we may write

$$x = a\tau^r + b$$

where $0 \leq b < \tau^r$ and $a \in \mathbb{Z}$. Now a is non-negative, because x is positive. Also, if $a \geq \tau$ then $\tau^{r+1} \leq x$ contrary to the definition of r, so $0 \leq a < \tau$.

(iii) Assume $x > 0$ has two τ-adic expansions

$$\begin{aligned} x &= a_0 + a_1\tau + a_2\tau^2 + \cdots + a_n\tau^n \\ &= b_0 + b_1\tau + b_2\tau^2 + \cdots + b_m\tau^m \end{aligned}$$

where $a_n \neq 0, b_m \neq 0$ and we may WLOG assume $n \leq m$. Now since

$$\begin{aligned} a_0 + a_1\tau + \cdots + a_n\tau^n &\leq (\tau - 1)\sum_{i=0}^{n} \tau^i \\ &= (\tau - 1)\frac{\tau^{n+1} - 1}{\tau - 1} \\ &= \tau^{n+1} - 1 \end{aligned}$$

we must have $n = m$ (since $m > n$ implies $x = \sum_i b_i\tau^i \geq \tau^{n+1}$). Using that $a_0 = [a_0]_\tau$ and $b_0 = [b_0]_\tau$ we see by division with τ that $a_0 = b_0$. But then

$$\tau(a_1 + a_2\tau + \cdots + a_n\tau^{n-1}) = \tau(b_1 + b_2\tau + \cdots + b_n\tau^{n-1})$$

and by induction we see that $a_i = b_i$ for all i; thus the τ-adic expansion of x is unique.

Ex. 1.6 Let $a = a_0 + a_1 \cdot 10^1 + \cdots + a_n \cdot 10^n$.

(i) Since 2 divides 10^k for $k \geq 1$, $a \equiv 0 \pmod 2$ if and only if $a_0 \equiv 0 \pmod 2$, that is if and only if 2 divides a_0.

(ii) Since 4 divides 10^k for $k \geq 2$, $4 \mid a$ if and only if $a \equiv 0 \pmod 4$ if and only if $a_0 + 10a_1 \equiv 0 \pmod 4$ if and only if $a_0 + 2a_1 \equiv 0 \pmod 4$.

(iii) As above, 8 divides 10^k for $k \geq 3$, and therefore $8 \mid a$ if and only if $a \equiv 0 \pmod 8$ if and only if $a_0 + 10a_1 + 100a_2 \equiv 0 \pmod 8$, and since $8 \mid 96$ this is equivalent to $a_0 + 2a_1 + 4a_2 \equiv 0 \pmod 8$.

(iv) As in (i), 5 divides 10^k for $k \geq 1$, and therefore 5 divides a if and only if 5 divides a_0.

(v) We have $10^k \equiv 1 \pmod 9$ for every $k \in \mathbb{N}$, and therefore $a \equiv 0 \pmod 9$ if and only if $a_0 + a_1 + \cdots + a_n \equiv 0 \pmod 9$, that is if and only if 9 divides the sum of the digits of a.

(vi) As above, $10^k \equiv 1 \pmod 3$, so $a \equiv 0 \pmod 3$ if and only if 3 divides the sum $a_0 + a_1 + \cdots + a_n$ of the digits of a.

(vii) Since $10 \equiv -1 \pmod{11}$, we have $10^k \equiv (-1)^k \pmod{11}$ for every $k \in \mathbb{N}$. Therefore $a \equiv 0 \pmod{11}$ if and only if $a_0 - a_1 + a_2 - \cdots \equiv 0 \pmod{11}$, ie. if and only if 11 divides the alternating sum of the digits.

(viii) To find a “divisibility rule” for division with 7 it is useful to build a table like this:

$$\begin{aligned}
10^0 &\equiv 1 \pmod 7\\
10^1 &\equiv 3 \pmod 7\\
10^2 &\equiv 2 \pmod 7\\
10^3 &\equiv -1 \pmod 7\\
10^4 &\equiv -3 \pmod 7\\
10^5 &\equiv -2 \pmod 7\\
10^6 &\equiv 1 \pmod 7
\end{aligned}$$

Thus $a = a_0 + 10a_1 + \cdots + 10^n a_n$ is divisible by 7 if and only if 7 divides the weighted sum $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \cdots$ of the digits of a, where the weights are continued periodically. The weights for a_3, a_4 and a_5 might of course also have been chosen to be 6, 4, and 5 respectively, but the choice made here makes it somewhat easier to remember the rule.

Ex. 1.7 We have (by the previous exercise) $233 \equiv 2 + 3 + 3 \equiv 2 \pmod 3$ and $577 \equiv 5 + 7 + 7 \equiv 1 \pmod 3$. Thus

$$233 \cdot 577 \equiv 2 \cdot 1 \equiv 2 \pmod 3.$$

But 3 divides 135441 since 3 divides $1+3+5+4+4+1 = 18$, and therefore $135441 \equiv 0 \pmod 3$, and thus $233 \cdot 577 = 135441$ is impossible.

Ex. 1.8 Since $4 \equiv 1 \pmod 3$, $4^n \equiv 1 \pmod 3$ for every $n \in \mathbb{N}$ by Proposition 1.3.4(ii). Thus $4^n - 1 \equiv 0 \pmod 3$, ie. $3 \mid 4^n - 1$.

Ex. 1.9 By definition, $\gcd(m,n)$ is the unique number $d \in \mathbb{N}$ for which $\operatorname{div}(d) = \operatorname{div}(m) \cap \operatorname{div}(n)$, so clearly $d \in \operatorname{div}(m) \cap \operatorname{div}(n)$. Since at least one of m, n is non-zero, at least one of the sets $\operatorname{div}(m)$ and $\operatorname{div}(n)$ is finite; thus the intersection is finite. d must be the largest element in this finite set, since no divisor of a positive number is larger than the number itself. Thus $d = \max \operatorname{div}(m) \cap \operatorname{div}(n)$.

Ex. 1.10 (i) Lemma 1.5.9 gives that there exist integers $\lambda, \mu, \lambda', \mu' \in \mathbb{Z}$ such that

$$d = \gcd(u,v) = \lambda u + \mu v \tag{1.4}$$

$$d' = \gcd(\tfrac{u}{2}, \tfrac{v}{2}) = \lambda' \tfrac{u}{2} + \mu' \tfrac{v}{2} \tag{1.5}$$

Now (1.5) implies $2d' = \lambda' u + \mu' v$, and since d is a divisor of both u and v, d divides the right-hand side. Thus d divides $2d'$.

On the other hand, (1.4) implies

$$\tfrac{d}{2} = \lambda \tfrac{u}{2} + \mu \tfrac{v}{2}$$

implying that $d' \mid \frac{d}{2}$, so that $2d'$ divides d. Now since both d and d' are positive we may conclude that $d = 2d'$.

(ii) Let $d = \gcd(u,v)$ and $d' = \gcd(\frac{u}{2}, v) = \lambda' \frac{u}{2} + \mu' v$. Then since v is odd, d is odd. Since d divides u and v, d also divides $\lambda' u + 2\mu' v = 2d'$. Now by Corollary 1.5.10 we see that d divides d'. On the other hand, d' divides v and $\frac{u}{2}$, hence it divides v and u, so we have in fact $d' \mid d$. We may conclude that $d = d'$.

(iii) An algorithm to find $\gcd(u,v)$ using the above results may be described as follows: First, if both u and v are even, divide them by 2 and "remember" how many times this is done. If one of the new numbers is even while the other is odd, use (ii) (as many times as possible). Now finally, if both numbers are odd, use the identity $\gcd(u,v) = \gcd(u, v-u)$; then $u - v$ is even and one may proceed as above. For example

$$\begin{aligned}
\gcd(336,140) &= 2\gcd(168,70)\\
&= 2^2\gcd(84,35)\\
&= 4\gcd(42,35)\\
&= 4\gcd(21,35)\\
&= 4\gcd(21,14)\\
&= 4\gcd(21,7)\\
&= 4 \cdot 7 = 28
\end{aligned}$$

Ex. 1.11 Let $x, y, z, d \in \mathbb{Z}$.

(i) Since $d \cdot 0 = 0$, d divides $0 = x - x$, so $x \equiv x \pmod{d}$.

(ii) If d divides $x - y$, then $ad = x - y$ for some $a \in \mathbb{Z}$. But then $(-a)d = -(x - y) = y - x$, so d divides $y - x$, ie. $y \equiv x \pmod{d}$.

(iii) If d divides $x - y$ and $y - z$, then $ad = x - y$ and $bd = y - z$ for some $a, b \in \mathbb{Z}$. Then $ad + bd = (a + b)d = x - z$, so d divides $x - z$; ie. $x \equiv z \pmod{d}$.

You may wish to compare the result of this exercise to Appendix A; according to Definition A.1.2(i) what we have shown is that $\equiv$ is in fact an equivalence relation on $\mathbb{Z}$.

Ex. 1.12 A few simple calculations yield

$$\begin{aligned}
34 &= 1 \cdot 89 - 1 \cdot 55 \\
21 &= 55 - 34 = -1 \cdot 89 + 2 \cdot 55 \\
13 &= 34 - 21 = 2 \cdot 89 - 3 \cdot 55 \\
8 &= 21 - 13 = -3 \cdot 89 + 5 \cdot 55 \\
5 &= 13 - 8 = 5 \cdot 89 - 8 \cdot 55 \\
3 &= 8 - 5 = -8 \cdot 89 + 13 \cdot 55 \\
2 &= 5 - 3 = 13 \cdot 89 - 21 \cdot 55 \\
1 &= 3 - 2 = -21 \cdot 89 + 34 \cdot 55,
\end{aligned}$$

from which it follows that $(\lambda, \mu) = (-21, 34)$ satisfies $89\lambda + 55\mu = 1$ and that $(-21) \cdot 89 \equiv 1 \pmod{55}$.

Consider the congruence

$$89x \equiv 7 \pmod{55}$$

Then $(-21 \cdot 89)x \equiv (-21) \cdot 7 \pmod{55}$, but since $(-21) \cdot 89 \equiv 1 \pmod{55}$ we have $x \equiv -147 \equiv 18 \pmod{55}$.

Now assume x is some number congruent to 18 modulo 55. Then $89x \equiv 89 \cdot 18 = 1602 \equiv 7 \pmod{55}$. Thus all solutions to the given congruence are numbers of the form $x = 18 + 55n$.

Ex. 1.13 Suppose $\lambda N + \mu M = d$, where $\lambda, \mu, M, N \in \mathbb{Z}$ and $N > 0$. Let μ' be the unique remainder obtained by dividing μ with N; ie. $\mu' = [\mu]_N$. Then

$\mu' = \mu - qN$ for some $q \in \mathbb{Z}$, and $0 \leq \mu' < N$. Inspired by the calculation $\mu' M = \mu M - qMN$ let $\lambda' = \lambda + qM$; then

$$\begin{aligned}\lambda' N + \mu' M &= (\lambda + qM)N + (\mu - qN)M \\ &= \lambda N + \mu M + qMN - qMN \\ &= d.\end{aligned}$$

Ex. 1.14 Let $d = \gcd(m, n)$. Thus d divides both m and n, and therefore d divides any linear combination of m and n. If there exists integers λ, μ such that $\lambda m + \mu n = 1$, d divides 1, and therefore d must equal 1, so m and n are relatively prime.

Ex. 1.15 Use induction on n and m. First we prove that $\gcd(a^m, b) = 1$ for every $m \in \mathbb{N}$. If $m = 0$ or $m = 1$ the result is trivial. Assume $\gcd(a^m, b) = 1$ for some $m \in \mathbb{N}$. The second half of Corollary 1.5.11 then gives that (since b is relatively prime to both a and a^m) $\gcd(a^{m+1}, b) = 1$, which proves that $\gcd(a^m, b) = 1$ for all $m \in \mathbb{N}$. The same procedure can be used to show that for a fixed $m \in \mathbb{N}$, $\gcd(a^m, b^n) = 1$ for every $n \in \mathbb{N}$, and since this holds for any m, the proof is complete.

Ex. 1.16 Let $m, n \in \mathbb{N}$ and let S denote the subset $\{xm + yn \mid x, y \in \mathbb{Z}\}$ of $\mathbb{Z}$.

(i) Let $q \in \mathbb{Z}$ and $s, t \in S$. Then $s = x_1 m + y_1 n$ and $t = x_2 m + y_2 n$ for suitable $x_i, y_i \in \mathbb{Z}$. Thus $qs = q(x_1 m + y_1 n) = (qx_1)m + (qy_1)n$, which shows that $qs \in S$. Furthermore $s + t = x_1 m + y_1 n + x_2 m + y_2 n = (x_1 + x_2)m + (y_1 + y_2)n$ which shows $s + t \in S$.

(ii) The assumption $S \neq \{0\}$ means that at least one of m, n is non-zero. One easily sees that this implies $S \cap \mathbb{N} \neq \emptyset$, so the definition

$$d = \min(S \cap \mathbb{N} \setminus \{0\})$$

is meaningful. From (i) it is clear that $\{ad \mid a \in \mathbb{Z}\} \subseteq S$.

Now let $t \in S$, and let r be the unique remainder (Theorem 1.2.1) obtained by division of t with d; thus $r = t - qd$ for some $q \in \mathbb{Z}$. Since t and $qd \in S$ it follows from (i) that $r \in S$. Now Theorem 1.2.1 guarantees that $0 \leq r < d$, and since d is the *smallest* positive element in S, r must equal 0. Thus d divides t and therefore $t \in \{ad \mid a \in \mathbb{Z}\}$, which shows the inclusion $\{ad \mid a \in \mathbb{Z}\} \subseteq S$; consequently

$$\{ad \mid a \in \mathbb{Z}\} = S.$$

(iii) Clearly d is a divisor in both m and n (since $m, n \in S = \{ad \mid a \in \mathbb{Z}\}$). Now since $d = xm + yn$ for some $x, y \in \mathbb{Z}$, it follows that if d' is another positive common divisor of m and n, then $d = xd'm' + yd'n'$, so that $d' \mid d$. Thus d is in fact the greatest common divisor of m and n. What we have shown is the following useful fact:

> Let $m, n \in \mathbb{Z}$, not both zero. Assume $d = \lambda m + \mu n$ is a positive integer dividing both m and n. Then $d = \gcd(m, n)$.

Ex. 1.17 The system of congruences

$$\begin{aligned} X &\equiv 2 \pmod 3 \\ X &\equiv 3 \pmod 5 \end{aligned}$$

has a unique solution modulo $3 \cdot 5 = 15$ by Theorem 1.6.4 (Chinese remainder theorem). Either with the construction of a "particular" solution as in Example 1.6.5 or by guessing, one finds that 8 is a solution. The smallest positive odd solution is therefore 23.

Ex. 1.18 A solution to the system of congruences

$$X \equiv 17 \pmod{504} \tag{1.6}$$
$$X \equiv -4 \pmod{35} \tag{1.7}$$
$$X \equiv 33 \pmod{16} \tag{1.8}$$

is easiest obtained by using the fact that two relatively prime integers m, n divide a third integer N if and only if their product divides N (Corollary 1.5.11 gives one half of this equivalence, the other half is obvious). Using that a congruence is really just a smart way of writing that a certain integer divides a difference of two integers, this gives that congruence (1.6) is equivalent to

$$X \equiv 17 \equiv 1 \pmod 8 \tag{1.9}$$
$$X \equiv 17 \equiv -1 \pmod 9 \tag{1.10}$$
$$X \equiv 17 \equiv 3 \pmod 7 \tag{1.11}$$

and the second congruence (1.7) is equivalent to

$$X \equiv -4 \equiv 1 \pmod 5 \tag{1.12}$$
$$X \equiv -4 \equiv 3 \pmod 7 \tag{1.13}$$

Now (1.11) is equivalent to (1.13), and therefore one is redundant. Furthermore (1.8) implies (1.9), so the latter is redundant. Thus the original system of congruences can be reduced to the equivalent system of congruences

$$\begin{aligned} X &\equiv 1 \pmod{16} \\ X &\equiv -1 \pmod{9} \\ X &\equiv 3 \pmod{7} \\ X &\equiv 1 \pmod{5} \end{aligned}$$

Since $5, 7, 9, 16$ are pairwise relatively prime, the Chinese remainder theorem gives a way of determining all integer solutions. Let $N = 5 \cdot 7 \cdot 9 \cdot 16 = 5040$. The construction of a solution in Theorem 1.6.4 requires us to find λ_i, μ_i satisfying

$$\begin{aligned} 5\lambda_1 + 1008\mu_1 &= 1 \\ 7\lambda_2 + 720\mu_2 &= 1 \\ 9\lambda_3 + 560\mu_3 &= 1 \\ 16\lambda_4 + 315\mu_4 &= 1. \end{aligned}$$

Without going through the details of finding solutions (qualified guesses are often the easiest way), one sees that

$$\begin{aligned} (\lambda_1, \mu_1) &= (605, -3) \\ (\lambda_2, \mu_2) &= (103, -1) \\ (\lambda_3, \mu_3) &= (249, -4) \\ (\lambda_4, \mu_4) &= (-59, 3) \end{aligned}$$

can be used. Thus a solution is

$$\begin{aligned} X &= 1 \cdot (-3) \cdot 1008 + 3 \cdot (-1) \cdot 720 + (-1) \cdot (-4) \cdot 560 + 1 \cdot 3 \cdot 315 \\ &= -1999 \end{aligned}$$

Any other integer which is congruent to -1999 modulo 5040 is also a solution, and all solutions are congruent to -1999 modulo 5040.

Ex. 1.19 We are given the information $0 \leq X < 60$, and

$$\begin{aligned} X &\equiv a \pmod{3} \\ X &\equiv b \pmod{4} \\ X &\equiv c \pmod{5} \end{aligned}$$

Since $3, 4, 5$ are pairwise relatively prime, X is uniquely determined modulo $3 \cdot 4 \cdot 5 = 60$; thus there is a unique number between 0 and 59 which satisfies the congruences. The weights $40, 45$ and 36 appear because of the equations

$$\begin{aligned} -13 \cdot 3 + 2 \cdot (60/3) &= 1 \\ -11 \cdot 4 + 3 \cdot (60/4) &= 1 \\ -7 \cdot 5 + 3 \cdot (60/5) &= 1 \end{aligned}$$

so that the Chinese remainder theorem gives that

$$X = 2 \cdot (60/3)a + 3 \cdot (60/4)b + 3 \cdot (60/5)c = 40a + 45b + 36c$$

is a solution. The number in question is thus the remainder obtained by dividing this (or any other) solution by 60.

Ex. 1.20 The number of eggs X satisfies according to the given information the congruences

$$\begin{aligned} X &\equiv 1 \pmod 2 && (1.14) \\ X &\equiv 1 \pmod 3 && (1.15) \\ X &\equiv 1 \pmod 4 && (1.16) \\ X &\equiv 1 \pmod 5 && (1.17) \\ X &\equiv 1 \pmod 6 && (1.18) \\ X &\equiv 0 \pmod 7. && (1.19) \end{aligned}$$

Now (1.16) implies (1.14), so the latter is redundant. Likewise (1.18) is equivalent to the set of congruences (1.14) and (1.15), so the first mentioned is redundant (as long as the latter two are satisfied). The above system of congruences is thus equivalent to

$$\begin{aligned} X &\equiv 1 \pmod 3 && (1.20) \\ X &\equiv 1 \pmod 4 && (1.21) \\ X &\equiv 1 \pmod 5 && (1.22) \\ X &\equiv 0 \pmod 7. && (1.23) \end{aligned}$$

Since $3, 4, 5,$ and 7 are pairwise relatively prime, the Chinese remainder theorem may be applied to obtain all solutions. As usual, let $N = 3 \cdot 4 \cdot 5 \cdot 7 = 420$. The algorithm requires us to find solutions to

$$\begin{aligned} 3\lambda_1 + 140\mu_1 &= 1 \\ 4\lambda_2 + 105\mu_2 &= 1 \\ 5\lambda_3 + 84\mu_3 &= 1 \\ 7\lambda_4 + 60\mu_4 &= 1. \end{aligned}$$

A possible set of solutions is

$$\begin{aligned}(\lambda_1, \mu_1) &= (47, -1)\\ (\lambda_2, \mu_2) &= (-26, 1)\\ (\lambda_3, \mu_3) &= (17, -1)\\ (\lambda_4, \mu_4) &= (-17, 2).\end{aligned}$$

Then a solution to the system (1.20)–(1.23) is

$$1 \cdot (-1) \cdot 140 + 1 \cdot 1 \cdot 105 + 1 \cdot (-1) \cdot 84 + 0 \cdot 2 \cdot 60 = -119,$$

and thus the smallest positive solution to the system of congruences is

$$X = -119 + 420 = 301.$$

301 is then the minimum number of eggs the old woman could have had.

Ex. 1.21 Let X denote the original number of coconuts, and let $f\colon x \mapsto \frac{4}{5}(x-1)$. Then the number of coconuts left after the first man has taken his share is $f(X)$, and the amount left after the n'th man has taken his is $X_n = f^{\circ n}(X)$. Now iteration of linear functions gives

$$\begin{aligned}f^{\circ n}(X) &= \left(\tfrac{4}{5}\right)^n X - \frac{4}{5}\left(\frac{1-(\frac{4}{5})^n}{1-\frac{4}{5}}\right)\\ &= \left(\tfrac{4}{5}\right)^n X - 4(1-(\tfrac{4}{5})^n)\\ &= \left(\tfrac{4}{5}\right)^n (X+4) - 4.\end{aligned}$$

Since X_5 must be an integer, and since 4 and 5 are relatively prime, 5^5 must divide $X + 4$. Thus in order for X_5 to be an integer, X must be at least $5^5 - 4 = 3121$. Putting $X = 3121$ one easily calculates

$$\begin{aligned}X_1 &= 2496\\ X_2 &= 1996\\ X_3 &= 1596\\ X_4 &= 1276\\ X_5 &= 1020\end{aligned}$$

which shows that if the initial amount of coconuts is 3121, there is an integer amount of coconuts congruent to 1 modulo 5 left after each of the first four men has taken their share, ie. 3121 is the desired number. The generalization of this problem and its solution is described at `http://mathworld.wolfram.com/MonkeyandCoconutProblem.html`.

Ex. 1.22 Let n be an odd integer. Then $\gcd(2,n)=1$, and by Proposition 1.7.1 we then have $\varphi(2n)=\varphi(2)\varphi(n)=\varphi(n)$.

Ex. 1.23 Let n be an integer ≥ 3. For any integer a it is true that $\gcd(a,n)=\gcd(n-a,n)$. This means in particular that

$$\gcd(a,n)=1 \Leftrightarrow \gcd(n-a,n)=1$$

Consider the sets $S_1=\{1,\ldots,\lfloor\frac{n}{2}\rfloor\}$ and $S_2=\{\lceil\frac{n}{2}\rceil,\ldots,n\}$.[1] We then have a 1–1-correspondence between integers relatively prime to n in S_1 and S_2, which shows that $\varphi(n)$ is even. [Observe that if there is a number $a\in S_1\cap S_2$ we must have $a=\frac{n}{2}$, but then $\gcd(n,a)=a\neq 1$, so there is no risk of counting a number coprime to n twice].

Ex. 1.24 One easily constructs the following table:

$$\begin{array}{rl}
2+1=3 & \text{prime}\\
2\cdot3+1=7 & \text{prime}\\
2\cdot3\cdot5+1=31 & \text{prime}\\
2\cdot3\cdot5\cdot7+1=211 & \text{prime}\\
2\cdot3\cdot5\cdot7\cdot11+1=2311 & \text{prime}\\
2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031 & \text{not prime}
\end{array}$$

since $30031=59\cdot509$. Thus in general one cannot expect $\prod_{n=1}^{N}p_n+1$ to be a prime number.

Ex. 1.25 Assume that n is not a prime number; ie. $n=ab$ where $a,b>1$. Then

$$\begin{aligned}
M_n &= 2^n-1\\
&= 2^{ab}-1\\
&= (2^a-1)\frac{(2^a)^b-1}{2^a-1}\\
&= (2^a-1)\sum_{i=0}^{b-1}(2^a)^i\\
&= (2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1)
\end{aligned}$$

which shows that M_n is composite and thus not a prime number. Thus in order for M_n to be a prime, n must be a prime.

The converse is *not* true, since for example $M_{11}=2^{11}-1=2047=23\cdot89$ is not a prime, though 11 is.

[1] Where $\lfloor\cdot\rfloor$ and $\lceil\cdot\rceil$ denotes "floor" and "ceiling", respectively.

Ex. 1.26 Assume $2^n + 1$ is a prime number. If n is not a power of 2, then n has some odd prime factor a; and $n = ab$. Then

$$2^n + 1 = (2^b + 1)(1 - 2^b + 2^{2b} - \cdots + 2^{(a-1)b}).$$

It is crucial that a is odd, since the sign of 2^{kb} in the second factor is $(-1)^k$. Thus $2^n + 1$ is not a prime if n is not a power of 2.

Let $F_n = 2^{2^n} + 1$. For $n = 0, \dots, 4$ the n'th Fermat numbers are $3, 5, 17, 257, 65537$, and these are easily seen to be prime numbers. The fifth Fermat number is not a prime, since $2^{2^5} + 1 = 641 \cdot 6700417$.

Ex. 1.27 As above, let $F_n = 2^{2^n} + 1$. Since $F_0 = 3 = 5 - 2 = F_1 - 2$, we have $\prod_{i=0}^{n-1} F_i = F_n - 2$ is true for $n = 1$. Now assume $\prod_{i=0}^{n-1} F_i = F_n - 2$ for some $n \geq 1$. Then

$$\begin{aligned}\prod_{i=0}^{n} F_i &= F_n \prod_{i=0}^{n-1} F_i \\ &= F_n(F_n - 2) \\ &= (2^{2^n} + 1)(2^{2^n} - 1) \\ &= 2^{2 \cdot 2^n} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2\end{aligned}$$

which shows that $\prod_{i=0}^{n} F_i = F_{n+1} - 2$ for all $n \in \mathbb{N}$.

If $m \neq n$ we may WLOG assume that $n > m$. Then $F_n - \prod_{i=0}^{n-1} F_i = 2$. If p is a prime dividing both F_n and F_m, p divides the left hand side, and thus p divides 2. Therefore $p = 2$ which is impossible, since all Fermat numbers are odd. Thus F_n and F_m are relatively prime if $m \neq n$.

Given any infinite subset A of $\mathbb{N}$ for which every pair of elements are relatively prime, one may easily prove that there are infinitely many primes. For if there were only N primes, choose $N+1$ different elements $x_1, \dots, x_{N+1}$ from A. For each of these, choose a prime factor p_i of x_i. Since the x_i are pairwise relatively prime, none of the p_i are equal; thus there are at least $N + 1$ primes, contrary to the hypothesis. Another more direct proof is this: Let $f\colon A \to \mathbb{P}$ be the mapping from A to the set of primes $\mathbb{P}$ which to an $x \in A$ associates the least prime factor of x; then f is injective, and since A is infinite, $\mathbb{P}$ is also infinite[2]. The above treatment of the set of Fermat numbers shows the existence of such a set A, so there are in fact infinitely many primes.

[2] Actually, f is not quite well-defined, if 0 or $1 \in A$. If one replaces A by $A' = \{x \in A \mid x \geq 2\}$ the argument works.

Ex. 1.28 Let $N = 2419$ and $S(x) = x^2 - N$. Since $49^2 = 2401 < 2419 < 2500 = 50^2$, $\lfloor\sqrt{2419}\rfloor = 49$. A few calculations gives

$$\begin{aligned} S(49) &= -18 \\ S(50) &= 81 = 9^2, \end{aligned}$$

and therefore $N = 50^2 - 9^2 = (50+9)(50-9) = 59 \cdot 41$, which is the desired prime factorization of 2419. These steps are easily carried out in less than three minutes.

Ex. 1.29 (i) Let $c = a^{p-2}$, and let b be the remainder obtained by dividing c by p. Then since $c \equiv b \pmod{p}$, $ac \equiv ab \pmod{p}$. Now $ac = a^{p-1}$, and since $1 < a < p-1$, p does not divide a, and from Fermat's little theorem we conclude that $a^{p-1} \equiv ab \equiv 1 \pmod{p}$.

By construction $0 \le b \le p-1$. Since p does not divide a, p does not divide $c = a^{p-2}$, so $b \neq 0$. If $b = 1$, we would have $ab = a \equiv 1 \pmod{p}$, which is absurd since $1 < a < p-1$. If $b = p-1$, $ab = ap - a \equiv -a \equiv 1 \pmod{p}$, ie. $a \equiv -1 \pmod{p}$ which again is a contradiction. Thus $1 < b < p-1$. If $b = a$, $a^2 \equiv 1 \pmod{p}$, so p divides $a^2 - 1 = (a+1)(a-1)$, and since p is a prime, p divides either $a+1$ or $a-1$, which again is absurd. Thus $a \neq b$.

To show that b is unique, assume $ab \equiv ab' \equiv 1 \pmod{p}$. Then p divides $ab - ab' = a(b-b')$, and since p does not divide a, p divides $b - b'$. Now $|b - b'| \le p-4$, we must have $b - b' = 0$.

(ii) For $p = 2$ we have $(2-1)! = 1 \equiv -1 \pmod{2}$. For $p = 3$ we also have $(3-1)! = 2 \equiv -1 \pmod{3}$. Now let p be a prime number > 3. Then

$$(p-1)! = (1 \cdot (p-1)) \cdot a_1 b_1 \cdots a_k b_k$$

where $k = (p-3)/2$ and the a_i are chosen to be the least number in the set $\{2, \ldots, p-2\}$ which does not already appear as a factor, and the corresponding b_i is chosen according to (i) so that $a_i b_i \equiv 1 \pmod{p}$. Since $p-1$ is even, it is clear that this procedure will give a rearrangement of the factors of $(p-1)!$. Using the product rule for congruences, one sees that

$$(p-1)! = (p-1)a_1 b_1 \cdots a_k b_k \equiv (-1) \cdot 1 \cdots 1 \equiv -1 \pmod{p}.$$

(iii) Assume $(n-1)! \equiv -1 \pmod{n}$ where $n \ge 2$. If n is not a prime, there are two possibilities: Either n may be written as a product of two distinct numbers a, b with $1 < a, b < n$, or n is a square. In the former case n is easily seen to divide $(n-1)!$, since both a and b appear as factors; thus $(n-1)! \equiv 0 \pmod{n}$ contrary to the original hypothesis. If n is not a prime and cannot be written as a product of two different numbers, n must be the square of some prime number p. If $p \geq 3$ both p and $2p$ appear as factors in $(n-1)!$, thus n divides $(n-1)!$, again contrary to the original hypothesis. The last remaining possibility is $n = 4 = 2^2$, but $(4-1)! = 6 \not\equiv -1 \pmod{4}$. To summarize: If

$$(n-1)! \equiv -1 \pmod{n}$$

and $n > 1$, n cannot be composite, and thus n must be a prime number.

Ex. 1.30 (i) By definition $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. Since

$$p \mid p! = i!(p-i)!\binom{p}{i}$$

and p does not divide $i!$ and $(p-i)!$ for $1 \leq i \leq p-1$, we conclude from Lemma 1.8.3 that $p \mid \binom{p}{i}$.

(ii) The binomial formula gives that

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

and since the terms corresponding to $i = 1, \ldots, p-1$ are divisible by p, one sees that

$$(a+b)^p \equiv \binom{p}{0} a^p + \binom{p}{p} b^p = a^p + b^p \pmod{p}.$$

(iii) If

$$n \mid \binom{n}{i} \quad \forall i \in \{1, 2, \ldots, n-1\}$$

then

$$\frac{(n-1)!}{i!(n-i)!} = \frac{(n-1)(n-2)\cdots(n-i+1)}{i!} \tag{1.24}$$

is an integer for all $i \in \{1, 2, \ldots, n-1\}$. If n is composite, let p be a prime factor of n. Obviously $2 \leq p \leq n-1$, so

$$\frac{(n-1)(n-2)\cdots(n-p+1)}{p!} = x$$

is an integer. But then

$$p(p-1)\cdots 2 \cdot 1 \cdot x = (n-1)(n-2)\cdots(n-p+1).$$

Now p is a prime dividing the left-hand side, so p divides one of the factors $n-1, n-2, \ldots, n-p+1$. But this is clearly impossible, since p *cannot* divide any of the integers between $n-p$ and n. Thus n cannot be composite and is therefore a prime number.

Ex. 1.31 (i) Assume $p_i = q_j$ for some i, j. Then $m' = \frac{m}{p_i}$ is a number which is smaller than m and has two different prime factorizations

$$\begin{aligned} m' &= p_1 \cdots p_{i-1} p_{i+1} \cdots p_r \\ &= q_1 \cdots q_{j-1} q_{j+1} \cdots q_s \end{aligned}$$

which contradicts m being the unique first element of M. Thus we may assume $\{p_1, \ldots, p_r\} \cap \{q_1, \ldots, q_s\} = \emptyset$.

(ii) Since $p_1 \neq q_1$ we may WLOG assume that $p_1 < q_1$. Then

$$n = p_1 \cdots p_r - p_1 q_2 \cdots q_s = m - p_1 q_2 \cdots q_s$$

is a positive integer less than m. Thus n has unique factorization (otherwise n would belong to M and m would not be the smallest element of M). Rewriting n a little, one sees that

$$\begin{aligned} n &= (q_1 - p_1) q_2 \cdots q_s \\ &= p_1 (p_2 \cdots p_r - q_2 \cdots q_s) \end{aligned}$$

Now since n has unique factorization, the prime p_1 must appear among the factors on the left hand side. From (i), p_1 cannot be any of $q_2, \ldots, q_s$. But if $p_1 = q_1 - p_1$ we have $q_1 = 2p_1$, so q_1 is not a prime. This contradicts n having a unique factorization, and thus contradicts M being non-empty.

Ex. 1.32 For any positive natural numbers a, b let $p_1, \ldots, p_k$ be the set of primes dividing either a or b (or both). Then a and b may be represented uniquely as

$$\begin{aligned} a &= p_1^{d_1} \cdots p_k^{d_k} \\ b &= p_1^{e_1} \cdots p_k^{e_k} \end{aligned}$$

where $d_k, e_k \geq 0$. Remark 1.8.6 then gives that

$$\gcd(a, b) = p_1^{\min(d_1, e_1)} \cdots p_k^{\min(d_k, e_k)}$$

and

$$\operatorname{lcm}(a, b) = p_1^{\max(d_1, e_1)} \cdots p_k^{\max(d_k, e_k)}.$$

Thus

$$\begin{aligned} \gcd(a, b) \operatorname{lcm}(a, b) &= p_1^{\min(d_1, e_1)} \cdots p_k^{\min(d_k, e_k)} \cdot p_1^{\max(d_1, e_1)} \cdots p_k^{\max(d_k, e_k)} \\ &= p_1^{d_1 + e_1} \cdots p_k^{d_k + e_k} \\ &= ab \end{aligned}$$

since $\min(d_i, e_i) + \max(d_i, e_i) = d_i + e_i$ for every pair of exponents. The product of the greatest common divisor and the least common multiple of two numbers is then the product of the two numbers.

Ex. 1.33 (i) Every divisor of n can be uniquely written as $p_1^{d_1} \cdots p_m^{d_m}$, where $0 \leq d_i \leq e_i$, and clearly all numbers that can be written this way are divisors of n. There are thus exactly $d(n) = (e_1 + 1) \cdots (e_m + 1)$ different divisors of n, since d_i may assume $e_i + 1$ different values independent of the other exponents, and different sets of exponents give different divisors (because of unique factorization).

(ii) We have

$$\frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1} = (1 + p_1 + \cdots + p_1^{e_1}) \cdots (1 + p_k + \cdots + p_k^{e_k})$$

and since every divisor of n may be written uniquely as a combination of exactly one term from each parentheses, one sees that multiplying out exactly gives the sum of the divisors of n, ie.

$$\frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1} = \sum_{d \in \operatorname{div}(n)} d$$

Ex. 1.34 Assume $2^{n+1}-1$ is a prime number p, and let $k = 2^n(2^{n+1}-1)$. Then the prime factorization of k is simply $2^n p$, and by Exercise 1.33 we may calculate $\sigma(k)$ as

$$\begin{aligned}\sigma(k) &= \frac{2^{n+1}-1}{2-1}\cdot\frac{p^2-1}{p-1}\\ &= (2^{n+1}-1)(p+1)\\ &= (2^{n+1}-1)2^{n+1}\\ &= 2k\end{aligned}$$

which shows that k is perfect.

Ex. 1.35 Searching Mathworld one finds the page `http://mathworld.wolfram.com/MersennePrime.html`, which states that the 36th Mersenne prime is $M_{36} = 2^{2976221}-1$ and that it has 895832 digits (in base 10). According to the previous exercise, $n = 2^{2976220}(2^{2976221}-1)$ is a perfect number, and it must have about 1.7 million digits.

Ex. 1.36 The numbers less than $n = p_1^{s_1}p_2^{s_2}$ which are not relatively prime to n are exactly the numbers which are multiples of either p_1 or p_2 (or both); the union of the two lists below are all such numbers:

$$\begin{aligned}0, p_1, 2p_1, \ldots, n-p_1 &= p_1(p_1^{s_1-1}p_2^{s_2}-1)\\ 0, p_2, 2p_2, \ldots, n-p_2 &= p_2(p_1^{s_1}p_2^{s_2-1}-1)\end{aligned}$$

To find the number of numbers *not* relatively prime to n, we must find how many of the above numbers have been counted twice. These are exactly the multiples of p_1p_2, ie.

$$0, p_1p_2, 2p_1p_2, \ldots, n-p_1p_2 = p_1p_2(p_1^{s_1-1}p_2^{s_2-1}-1)$$

Counting the number of numbers in the above lists one finds that $\varphi(n)$ may be expressed as

$$\begin{aligned}\varphi(n) &= n - p_1^{s_1-1}p_2^{s_2} - p_1^{s_1}p_2^{s_2-1} + p_1^{s_1-1}p_2^{s_2-1}\\ &= p_1^{s_1}p_2^{s_2} - p_1^{s_1-1}p_2^{s_2} - p_1^{s_1}p_2^{s_2-1} + p_1^{s_1-1}p_2^{s_2-1}\\ &= (p_1^{s_1}-p_1^{s_1-1})(p_2^{s_2}-p_2^{s_2-1}).\end{aligned}$$

Ex. 1.37 One easily sees

$$\begin{aligned}F_5 &= 2^{2^5}+1 = 2^{32}+1\\ &= 2^4(2^7)^4+1 = (5^4+2^4)(2^7)^4 - 5^4(2^7)^4+1.\end{aligned}$$

Furthermore $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$. Since $1 + x$ divides $1 - x^4$:

$$(1 + x)(1 - x + x^2 - x^3) = 1 - x^4,$$

putting $x = 5 \cdot 2^7$ one sees that 641 divides both $(5^4 + 2^4)(2^7)^4$ and $1 - 5^4(2^7)^4$; thus 641 divides F_5 which is therefore not prime. The quotient $F_5/641 = 6700417$ is a prime, so F_5 only has two prime factors.

Ex. 1.38 Since p and q are unequal, $\varphi(N) = (p - 1)(q - 1) = pq - (p + q) + 1$. Then the equation becomes

$$X^2 - (p + q)X + pq = 0$$

and either by direct substitution or by using the fact from calculus that the product of the roots of a monic second degree polynomial is the constant term and the sum is the coefficient of the linear term with opposite sign, one sees that p and q are (the) roots.

If somehow $\varphi(N)$ could be computed easily, we could certainly easily find the roots of the polynomial $X^2 + (\varphi(N) - N - 1)X + N$, ie. factoring N would be easy (provided we know N is the product of two distinct primes).

Ex. 1.39 The necessary computations are impossible to do by hand, but a small *Mathematica* program easily calculates the encoded message:

```
p = ⟨first prime⟩;
q = ⟨second prime⟩;
RSA129 = p*q;
publicexponent = 9007;
publicmessage = ⟨the encoded published message⟩;
mu = ExtendedGCD[(p-1)(q-1), publicexponent][[2,2]];
d = Mod[mu,(p-1)(q-1)];
toLetter[0]=" ";
toLetter[n_Integer] := FromCharacterCode[n + 64];
SetAttributes[toLetter, Listable];
origmessage = PowerMod[publicmessage, d, RSA129];
StringJoin[toLetter[Mod[Quotient[origmessage, 10^#],
   100]] &@ Range[Floor[Log[10, origmessage]] - 1, 0,
   -2]]
```

The tokens ⟨*some text*⟩ should of course be substituted by the appropriate numbers. The first couple of lines simply define some variables. The trailing ; suppresses output from these lines. The `ExtendedGCD[a,b]` returns a list $\{\gcd(a,b),\{\lambda,\mu\}\}$; we are only interested in the μ, and the `[[2,2]]`-construction extracts the second element of the second element of the preceding list. To make sure $0 \leq d < \varphi(\texttt{RSA129}) = (p-1)(q-1)$ we define `d` using `Mod`. The `toLetter` function gives a one-character string according to the given encoding, and the `SetAttributes` makes it possible to "thread" `toLetter` over a list of integers. The original message (as a number) is then calculated using the very efficient `PowerMod`. The last line looks frightening at first, but what is being done is simply this: Construct a list of the even numbers from 0 up to the numbers of digits in `origmessage` minus 2, in decreasing order. This makes it possible to extract the digits of `origmessage` two by two using `Quotient` and `Mod`; and applying `toLetter` to each of these. The `StringJoin` simply takes a list of strings and concatenates them, so the result is the encoded original message. When running the above lines, the output is this:

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

which is thus the message originally encrypted in 1977.

Ex. 1.41 Assume $\gcd(a,N) > 1$ for $a,N \in \mathbb{Z}$ and $N \geq 1$. If $N = 1$ the assumption $\gcd(a,N) > 1$ is false, so we may assume $N \geq 2$. Then if $a^{N-1} \equiv 1 \pmod{N}$ we have $a^{N-1} - 1 = kN$ for some $k \in \mathbb{Z}$, and then $a^{N-2}a + (-k)N = 1$, so $\gcd(a,N) = 1$, contrary to the hypothesis. Thus $a^{N-1} \not\equiv 1 \pmod{N}$.

Ex. 1.42 Assume $p = 899$ is a prime number. Then since p does not divide 2, Fermat's little theorem gives that

$$2^{898} \equiv 1 \pmod{899}.$$

But a relatively simple calculation shows that $2^{898} \equiv 845 \pmod{899}$, which is not congruent to 1 modulo 899. This calculation can either be done using a computer[3] or by hand using the repeated squaring algorithm. Thus 899 can not be a prime number.

[3] With a computer running Linux, the easiest way is probably to execute `echo "2 898 899 | p" | dc` at a prompt. `dc` is an arbitrary precision reverse-polish calculator which is part of most GNU/Linux-distributions. This command means "send the string `2 898 899 | p` to `dc`"; `dc` then reads this and pushes 2, 898, and 899 on the stack; the `|` tells `dc` to perform modular exponentiation on the three topmost numbers on the stack, and push the result on the stack. The `p` prints the value of the topmost number to stdout. The quotes `"` are necessary in order that the shell makes the first vertical bar a part of the string.

Ex. 1.43 Assume $p = 15$ is a prime, and let $k = 1$ and $q = 7$ such that $p-1 = 14 = 2^k \cdot q$; let in addition $a = 11$. Then using the repeated squaring algorithm we find

$$\begin{aligned}\left[11^7\right]_{15} &= \left[[11^4][11^2][11]\right] \\ &= \left[[11^2]^2 \cdot 1 \cdot 11\right] \\ &= [11]\end{aligned}$$

such that $11^7 \not\equiv 1 \pmod{15}$. Furthermore we see immediately that $11^7 \not\equiv -1 \pmod{15}$. Then Proposition 1.9.6 states that we must have $11^{14} \equiv -1 \pmod{15}$. But

$$\begin{aligned}\left[11^{14}\right]_{15} &= \left[[11^7]^2\right] \\ &= [11^2] \\ &= [1]\end{aligned}$$

so that $11^{14} \not\equiv -1 \pmod{15}$. Thus the assumption that 15 is a prime cannot be true; and 15 is not a strong pseudoprime relative to 11.

Ex. 1.44 Let $p = 25$ and $a = 7$. Then $p - 1 = 2^3 \cdot 3$, and $7^3 = 343 \equiv 18 \not\equiv \pm 1 \pmod{25}$. But

$$7^6 = 117649 \equiv -1 \pmod{25}$$

so according to Definition 1.9.5 25 is a strong pseudoprime relative to 7.

Ex. 1.45 Let $n = p_1 \cdots p_r$ be a product of distinct primes, and suppose that $p_i - 1 \mid n - 1$ for all i.

(i) If $\gcd(a, n) = 1$, then certainly $\gcd(a, p_i) = 1$ for all $i = 1, \ldots, r$. Then by Fermat's little theorem

$$\begin{aligned}a^{p_1-1} &\equiv 1 \pmod{p_1} \\ &\vdots \\ a^{p_r-1} &\equiv 1 \pmod{p_r}.\end{aligned}$$

Since $p_i - 1 \mid n - 1$ for all i, we may find s_i such that $s_i(p_i - 1) = n - 1$. Thus we also have

$$\begin{aligned}(a^{p_1-1})^{s_1} = a^{n-1} &\equiv 1 \pmod{p_1} \\ &\vdots \\ (a^{p_r-1})^{s_r} = a^{n-1} &\equiv 1 \pmod{p_r}.\end{aligned}$$

Since the p_i are distinct, they are relatively prime, and Corollary 1.5.11(i) then shows that

$$a^{n-1} \equiv 1 \pmod{n}.$$

(ii) We may write 561 as $3 \cdot 11 \cdot 17$. It is easily checked that 2, 10, and 16 divides 560, and from (i) we have that 561 is then pseudoprime to every base a which is relatively prime to 561, and is thus a Carmichael number.

(iii) 1105 is also a Carmichael number, since $1105 = 5 \cdot 13 \cdot 17$ and $4, 12, 16$ all divide 1104. Another example is $1729 = 7 \cdot 13 \cdot 19$, since $6, 12, 18$ divide 1728. It can be shown that if $6k+1, 12k+1, 18k+1$ are all prime, then their product is a Carmichael number; 1729 is an example of such a number. See `http://mathworld.wolfram.com/CarmichaelNumber.html`.

Ex. 1.46 A very simple way of implementing Pollard's ρ-algorithm in Mathematica is this:

```
n = 10403;
f[X_] := Mod[X^2 + 1, n];
X[0] = Y[0] = 0;
X[i_] := f[X[i - 1]]; Y[i_] := f[f[Y[i - 1]]];
i = 0;
While[GCD[X[i] - Y[i], n] == 1 || GCD[X[i] - Y[i], n]
   == n, i++];
i
GCD[X[i] - Y[i], n]
```

It turns out that for this particular value of n, the algorithm halts when $i = 14$, and $\gcd(X_{14} - Y_{14}, 10403) = 103$. Thus 103 is a non-trivial factor of 10403, which may thus be factored as $10403 = 103 \cdot 101$. Since 101 is the 26'th prime, trial division would have required approximately twice as many steps. The values of the X_i and Y_i can be seen in this table:

i	0	1	2	3	4	5	6	7	8	9
X_i	0	1	2	5	26	677	598	3903	3418	156
Y_i	0	2	26	598	3418	3531	3724	9812	9970	3682
gcd	10403	1	1	1	1	1	1	1	1	1

i	10	11	12	13	14
X_i	3531	5168	3724	978	9812
Y_i	7087	2594	4973	943	3632
gcd	1	1	1	1	103

Ex. 1.47 An implementation of Pollard's ρ-algorithm which doesn't offer the ability to print a table of X_i, Y_i is this:

```
n = 2^(2^8) + 1;
f[X_] := PowerMod[X, 2048, n] + 1;
Xi = Yi = 3;
While[GCD[Xi - Yi, n] == 1 || GCD[Xi - Yi, n] == n,
   Xi = f[Xi]; Yi = f[f[Yi]]];
GCD[Xi - Yi, n]
```

After 1321444 recursion steps this method returns the divisor $p = 1238926361552897$. Then the factorization of $2^{2^8} + 1$ is

$$1238926361552897 \cdot$$
$$93461639715357977769163558199606896584051237541638188580280321;$$

both of these are primes. According to `http://mathworld.wolfram.com/FermatNumber.html` Pollard was the first to factor F_8.

Ex. 1.48 Let $N = 295927$, $a = 2$ and $B = 6$; thus the primes we will consider are 2, 3, and 5. We calculate

$$\begin{aligned}\lceil \log_2 \sqrt{N} \rceil &= 10 \\ \lceil \log_3 \sqrt{N} \rceil &= 6 \\ \lceil \log_5 \sqrt{N} \rceil &= 4\end{aligned}$$

Then $m = 2^{10}3^6 5^4 = 466560000$. Using a fast algorithm such as repeated squaring, `echo "2 466560000 295927 | p" | dc` or the function `PowerMod` in Mathematica, we then find

$$[2^{466560000}]_{295927} = 277534$$

and the Euclidean algorithm gives $\gcd(295927, 277533) = 541$. Thus 541 is a non-trivial factor of N, and the complete factorization is $541 \cdot 547$.

Ex. 1.49 (i) Let $x = p_1^{m_1} \cdots p_r^{m_r}$ be a prime factorization, where $p_i \neq p_j$ for $i \neq j$. Clearly if all of the m_i are even, we may write $m_i = 2n_i$ and then

$$\begin{aligned}x &= p_1^{m_1} \cdots p_r^{m_r} \\ &= p_1^{2n_1} \cdots p_r^{2n_r} \\ &= (p_1^{n_1} \cdots p_r^{n_r})^2\end{aligned}$$

so x is a square.

Now assume x is a square. Then we may write $x = y^2$ for some positive integer y. Let $y = q_1^{n_1} \cdots q_s^{n_s}$ be the prime factorization of y, where as usual $q_i \neq q_j$. Now every prime dividing y must divide x. But on the other hand, if a prime divides x, it divides $y^2 = y \cdot y$, so by Lemma 1.8.3 it divides y. Thus we have $s = r$ and we may write $p_1 = q_1, \ldots, p_r = q_r$. Now $y^2 = (p_1^{n_1} \cdots p_r^{n_r})^2 = p_1^{2n_1} \cdots p_r^{2n_r} = p_1^{m_1} \cdots p_r^{m_r}$, and by the uniqueness of prime factorization we must have $m_1 = 2n_1, \ldots, m_r = 2n_r$; thus all exponents are even.

(ii) Consider the $r \times n$ matrix $A = [m_{ij}]$. Reducing all entries modulo 2, ie. writing a 0 if m_{ij} is even and a 1 if m_{ij} is odd, we may consider A as a matrix in $\mathrm{Mat}_{r,n}(\mathbb{F}_2)$. The idea is now that $a_{i_1} \cdots a_{i_s}$ is a square exactly when all of the exponents are even. Let v denote the vector in ${\mathbb{F}_2}^n$ which has 1's at positions $i_1, \cdots, i_s$ and 0's otherwise. Then $a_{i_1} \cdots a_{i_s}$ is a square if and only if $Av = 0$, since the vector Av is a $r \times 1$ vector indicating the parity of the exponents of $p_1, \cdots, p_r$. Of course $v = 0$ is a solution, corresponding to the empty product of a_i's, which by definition is 1 (a square). We may then conclude that a non-trivial solution exists if and only if $\operatorname{Ker} A \neq \{0\}$. Now if $n > r$ we know from linear algebra that a non-trivial solution must exist (since $\mathbb{F}_2$ is finite, it is quite easy to prove: $A \colon {\mathbb{F}_2}^n \to {\mathbb{F}_2}^r$ cannot be injective, so we may find $v_1 \neq v_2$ such that $Av_1 = Av_2$; then by linearity $A(v_1 - v_2) = 0$ and $v_1 - v_2 \neq 0$). If $n \leq r$ one may row-reduce A to determine whether non-trivial solutions exist or not.

Ex. 1.50 Let $f(X) = a_n X^n + \cdots + a_1 X + a_0$, where $a_i \in \mathbb{Z}$.

(i) For all $n \in \mathbb{N}$, $n \geq 2$ we have the factorization

$$X^n - a^n = (X - a)(X^{n-1} + X^{n-2}a + \cdots + Xa^{n-2} + a^{n-1})$$

for all $X, a \in \mathbb{Z}$, so $X - a \mid X^n - a^n$. If $n = 1$ trivially $X - a \mid X - a$, and for $n = 0$ we have $X - a \mid X^0 - a^0 = 0$.

(ii) Let $a, N \in \mathbb{Z}$ and assume that $N \nmid a_n$. Assume $f(a) \equiv 0 \pmod{N}$. Then $f(X) \equiv f(X) - f(a) \pmod{N}$, and we may write

$$\begin{aligned} f(X) - f(a) &= a_n(X^n - a^n) + \cdots + a_1(X - a) + a_0(X^0 - a^0) \\ &= a_n(X^n - a^n) + \cdots + a_1(X - a) \end{aligned}$$

Then since $X - a$ divides each term, $X - a$ divides $f(X) - f(a)$. Thus

$$\begin{aligned} f(X) &\equiv f(X) - f(a) \\ &= (X - a)g(X) \pmod{N} \end{aligned}$$

where $g(X)$ is chosen appropriately. Now it follows from the factorization in (i) that the degree of g is $n-1$, and a little consideration reveals that the coefficient of X^{n-1} is a_n; thus the degree of g modulo N is $n - 1$.

(iii) Let p be a prime, and f a polynomial of degree 1 modulo p. Then $f(X) = a_1X + a_0$ where $p \nmid a_1$. Assume the existence of two solutions X_1, X_2 to $f(X) \equiv 0 \pmod{p}$. Then $a_1X_1 + a_0 \equiv a_1X_2 + a_0 \pmod{p}$ and $a_1(X_1 - X_2) \equiv 0 \pmod{p}$. Since p does not divide a_1, p divides $X_1 - X_2$, so X_1 and X_2 are congruent modulo p.

Now assume the statement is true for all polynomials of degree at most $n - 1$. Let f be a polynomial of degree n modulo p. If X_0 is some solution to $f(X) \equiv 0 \pmod{p}$, we may write $f(X) \equiv (X - X_0)g(X) \pmod{p}$ where g has degree $n - 1$ modulo p. If X is any solution to $f(X) \equiv 0 \pmod{p}$, then either $X - X_0 \equiv 0 \pmod{p}$ or $g(X) \equiv 0 \pmod{p}$. By induction hypothesis there are at most $n - 1$ pairwise incongruent solutions the the latter congruence, while the former has exactly one solution. Thus in all there are no more than n pairwise incongruent solutions modulo p.

This is not true if p is not a prime. For consider the polynomial $f(X) = 2X$. f clearly has degree 1 modulo 4, but the congruence $f(X) \equiv 0 \pmod{4}$ has the incongruent solutions $X = 2$ and $X = 4$.

Ex. 1.51 Let p be an odd prime. Then directly from Corollary 1.11.5:

(i) If a and b are quadratic residues, $(\frac{a}{p}) = (\frac{b}{p}) = 1$ and therefore $(\frac{ab}{p}) = 1$.

(ii) If a and b are quadratic non-residues, $(\frac{a}{p}) = (\frac{b}{p}) = -1$ and therefore $(\frac{ab}{p}) = 1$.

(iii) If a is a quadratic residue and b is a quadratic non-residue, $(\frac{a}{p}) = 1$ and $(\frac{b}{p}) = -1$, so $(\frac{ab}{p}) = -1$.

Part (i) may also be proved in a somewhat constructive way, for if a and b are quadratic residues modulo p, there exists x, y such that $x^2 \equiv a \pmod{p}$ and $y^2 \equiv b \pmod{p}$; thus $x^2y^2 = (xy)^2 \equiv ab \pmod{p}$, so there exists a solution to the congruence $z^2 \equiv ab \pmod{p}$.

Ex. 1.52 Since there are $(13-1)/2 = 6$ quadratic residues, and since $i^2 \equiv (13-i)^2 \pmod{13}$ we may find them by calculating the residues of $1^2, \ldots, 6^2$ modulo 13. These are

$$1, 4, 9, 3, 12, 10$$

so the quadratic non-residues modulo 13 must be

$$2, 5, 6, 7, 8, 11.$$

Ex. 1.53 Let p be a prime $\equiv 1 \pmod{12}$. Writing $p = 12k+1$ and using the law of quadratic reciprocity we have

$$\begin{aligned}\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) &= (-1)^{\frac{3-1}{2}\frac{p-1}{2}} \\ &= (-1)^{6k} \\ &= 1\end{aligned}$$

Now since $(\frac{p}{3}) = (\frac{12k+1}{3}) = (\frac{1}{3}) = 1$ since $1^2 \equiv 1 \pmod 3$, we have $\left(\frac{3}{p}\right) = 1$, so 3 is a quadratic residue modulo p.

Ex. 1.54 Using the law of quadratic reciprocity, we have

$$\begin{aligned}\left(\frac{7}{17}\right) &= \left(\frac{17}{7}\right) \\ &= \left(\frac{3}{7}\right) \\ &= -\left(\frac{7}{3}\right) \\ &= -\left(\frac{1}{3}\right) \\ &= -1\end{aligned}$$

so 7 is a quadratic non-residue modulo 17 (and vice versa).

Chapter 2

Ex. 2.1 Let G be a group and $g \in G$. Define the map $\xi\colon G \to G$ by $\xi(x) = xg$. We wish to show that ξ is bijective. Now let $y \in G$. We wish to find an x such that $\xi(x) = y$. Define $x = yg^{-1}$; then $\xi(x) = (yg^{-1})g = y(g^{-1}g) = ye = y$, so ξ is surjective. Here the existence of an inverse element (axiom iii), the associativity (axiom i), and the property of the neutral element e (axiom ii) was all used.

Now assume $\xi(x_1) = \xi(x_2)$; ie. $x_1g = x_2g$. Multiplying both sides with g^{-1} from the right we have $x_1 = x_2$, so ξ is injective. Again all three axioms were necessary. Since ξ is both surjective and injective, it is bijective.

Another proof following the same idea as in §2.1.6 is defining the map $\psi\colon G \to G$ by $\psi(x) = xg^{-1}$, which by computation is seen to be ξ^{-1}, the inverse map of ξ.

Ex. 2.2 Let the four elements be denoted e, a, b and c, where e is the neutral element. The composition table must start like

$\circ$	e	a	b	c
e	e	a	b	c
a	a		X	
b	b			
c	c			

.

Now §2.1.6 states that each row and each column in the composition table contains exactly one occurrence of each of the four elements. The entry marked with an X must therefore be either e or c. In the former case the "jigsaw" has only the solution

$\circ$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

(2.1)

and in the latter one finds that the composition table must be completed as

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

or

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

or

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Taking a closer look at the latter two of these, and comparing them with the composition table (2.1), one sees that they actually represent the same group; one element besides e is its own inverse, and when this element is determined the composition table is determined. Given any group of order 4 which matches any of these three composition tables, one may (re)name the elements of the group to match the other two.

One may conclude that for a group of order 4, there are only two (essentially different) possible composition tables.

Ex. 2.4 Assume $H \subseteq G$ is a subgroup of G. Then for each element $y \in H$ we have $y^{-1} \in H$. Since H is closed under the composition from G, $x, y \in H$ implies that $xy^{-1} \in H$.

Now assume $xy^{-1} \in H$ for all $x, y \in H$. Since H is non-empty, we may choose an element $x \in H$, and using the assumption (with $x = y$) we see that $xx^{-1} = e \in H$, so that H contains the neutral element. If y is any element in H, the assumption (with $x = e$) gives that $ey^{-1} = y^{-1} \in H$, such that every element in H has an inverse in H. Finally, if x and y are elements of H, $y^{-1} \in H$, and using the assumption on the pair x, y^{-1} one sees that $x(y^{-1})^{-1} = xy \in H$, such that H is closed under the composition from G. Thus H is a subgroup of G.

Ex. 2.5 Assume $H \subseteq G$ is a finite non-empty subset of G, and that $xy \in H$ for $x, y \in H$. Choose an element $x \in H$. Then $x^2 \in H$, and by induction $x^n \in H$ for every $n \in \mathbb{N} \setminus \{0\}$. Since H is finite, not all of these are distinct. Thus we may find i, j with $i < j$ such that $x^i = x^j$. But then $x^{j-i}x^i = x^j = x^i$ which means that $x^{j-i} = e$, so $e \in H$.

For any element $x \in H$ we may find such a pair i, j, and then $x \circ x^{j-i-1} = x^{j-i} = e$, which means that $x^{-1} = x^{j-i-1} \in H$. Finally H was assumed to be closed under the composition from G, so H is a subgroup of G.

A simple example that the above breaks down if H is not finite is the additive group $G = (\mathbb{Z}, +)$. Let $H = (\mathbb{N}, +)$. Then clearly H is closed under addition, but since $-1 \notin \mathbb{N}$, H is not a subgroup of G.

Ex. 2.6 Consider the set $\mathrm{GL}_2(\mathbb{R})$ of 2×2-matrices with real entries and non-zero determinant. We wish to show that $\mathrm{GL}_2(\mathbb{R})$ with matrix multiplication as composition is a group. Now it is well known from linear algebra that $\det AB = \det A \det B$, so clearly $\mathrm{GL}_2(\mathbb{R})$ is closed under multiplication. The 2×2 identity matrix I serves as neutral element since $IA = AI = A$ for all $A \in \mathrm{GL}_2(\mathbb{R})$. Finally, another fact from linear algebra is that a 2×2-matrix is invertible if and only if its determinant is non-zero. We also have

$\det(A^{-1}) = (\det A)^{-1}$, so $\det(A^{-1}) \neq 0$ implying $A^{-1} \in \mathrm{GL}_2(\mathbb{R})$. Thus $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ is in fact a group. It is non-abelian, since for instance

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

In exactly the same way one may prove that $O_2(\mathbb{R})$, the set of all 2×2 orthogonal matrices, is a group. An example of two orthogonal matrices which do not commute is

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Ex. 2.7 Let $N = \{e, d, f\}$. Then it is easy to check that N is a subgroup of S_3 ($d^2 = f$, $f^2 = d$, and $fd = df = e$). Clearly then $gNg^{-1} = N$ for $g = e, d, f$. Using the composition table, one may verify that $ada^{-1} = f$, and that this is also true if a is replaced by b or c, and if d and f are interchanged. Thus $gNg^{-1} = N$ for all $g \in S_3$, so that N is normal. Note that this result may also be proved using Exercise 15(iii) (since $[S_3 : N] = 6/3 = 2$ by Theorem 2.2.8 (Lagrange)).

The subgroups of order two consist of the neutral element and an element which is its own inverse. From the composition table it is clear that there are three such subgroups, namely $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$. None of these are normal, since for instance $bab^{-1} = c \notin \{e, a\}$, and in a similar fashion one may show that the other two are not normal.

Ex. 2.8 Let $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ be a linear isometry.

(i) Using the formula $|v - w|^2 = |v|^2 + |w|^2 - 2v \cdot w$ twice and that φ is a linear isometry, we see that

$$\begin{aligned} 2\varphi(v_1) \cdot \varphi(v_2) &= |\varphi(v_1)|^2 + |\varphi(v_2)|^2 - |\varphi(v_1) - \varphi(v_2)|^2 \\ &= |v_1|^2 + |v_2|^2 - |v_1 - v_2|^2 \\ &= 2v_1 \cdot v_2 \end{aligned}$$

(ii) By (i), φ preserves the inner product of two vectors. In particular $\varphi(e_1) \cdot \varphi(e_2) = e_1 \cdot e_2 = 0$. Then clearly $\varphi(e_1), \varphi(e_2)$ is an orthonormal basis for $\mathbb{R}^2$. Now

$$\begin{aligned}\varphi(\lambda e_1 + \mu e_2) \cdot \varphi(e_1) &= (\lambda e_1 + \mu e_2) \cdot e_1 = \lambda \\ \varphi(\lambda e_1 + \mu e_2) \cdot \varphi(e_2) &= (\lambda e_1 + \mu e_2) \cdot e_2 = \mu\end{aligned}$$

so in the basis $\{\varphi(e_1), \varphi(e_2)\}$ we may write

$$\varphi(\lambda e_1 + \mu e_2) = \lambda\varphi(e_1) + \mu\varphi(e_2)$$

(iii) Let $v \in \mathbb{R}^2$ and $\lambda \in \mathbb{R}$. Writing v in the standard basis $\{e_1, e_2\}$ we have

$$\begin{aligned}\varphi(\lambda v) &= \varphi(\lambda(a_1e_1 + a_2e_2)) \\ &= \varphi(\lambda a_1e_1 + \lambda a_2e_2) \\ &= \lambda a_1\varphi(e_1) + \lambda a_2\varphi(e_2) \\ &= \lambda(a_1\varphi(e_1) + a_2\varphi(e_2)) \\ &= \lambda\varphi(v)\end{aligned}$$

Now let $v_1 = (a_1, a_2)$ and $v_2 = (b_1, b_2)$ in the standard basis $\{e_1, e_2\}$. Then as above we have

$$\begin{aligned}\varphi(v_1 + v_2) &= \varphi(a_1e_1 + a_2e_2 + b_1e_1 + b_2e_2) \\ &= \varphi((a_1 + b_1)e_1 + (a_2 + b_2)e_2) \\ &= (a_1 + b_1)\varphi(e_1) + (a_2 + b_2)\varphi(e_2) \\ &= a_1\varphi(e_1) + a_2\varphi(e_2) + b_1\varphi(e_1) + b_2\varphi(e_2) \\ &= \varphi(v_1) + \varphi(v_2)\end{aligned}$$

(iv) The matrix representation of φ in the basis $\{e_1, e_2\}$ is

$$\begin{pmatrix} | & | \\ \varphi(e_1) & \varphi(e_2) \\ | & | \end{pmatrix}$$

and the transpose of this matrix is

$$\begin{pmatrix} -\varphi(e_1)- \\ -\varphi(e_2)- \end{pmatrix}.$$

The product of these matrices is

$$\begin{pmatrix} \varphi(e_1) \cdot \varphi(e_1) & \varphi(e_1) \cdot \varphi(e_2) \\ \varphi(e_2) \cdot \varphi(e_1) & \varphi(e_2) \cdot \varphi(e_2) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

since φ preserves the length of a vector. Thus the determinant of φ is non-zero (it is in fact ±1), so φ is invertible. This fact may also be seen simply by looking at $\operatorname{Ker}\varphi = \{0\}$, since $\varphi(v) = 0 \Leftrightarrow v = 0$, and since φ is a linear map from $\mathbb{R}^2$ to $\mathbb{R}^2$, it must be bijective.

Ex. 2.9 (i) The elements of G may be listed as

- The identity $\mathrm{Id} = \mathrm{Id}_{\mathbb{R}^2}$
- Rotations of $\pm\pi/2$ around 0, R_+, R_-.
- A rotation of π around 0, R_π.
- Reflections in the coordinate axes, R_x, R_y.
- Reflections in the diagonals $x = y$ and $x = -y$, R_1, R_2.

(ii) With the above notation the composition table for G is

$\circ$	Id	R_+	R_-	R_π	R_x	R_y	R_1	R_2
Id	Id	R_+	R_-	R_π	R_x	R_y	R_1	R_2
R_+	R_+	R_π	Id	R_-	R_2	R_1	R_y	R_x
R_-	R_-	Id	R_π	R_+	R_1	R_2	R_x	R_y
R_π	R_π	R_-	R_+	Id	R_y	R_x	R_2	R_1
R_x	R_x	R_1	R_2	R_y	Id	R_π	R_+	R_-
R_y	R_y	R_2	R_1	R_x	R_π	Id	R_-	R_+
R_1	R_1	R_y	R_x	R_2	R_-	R_+	Id	R_π
R_2	R_2	R_x	R_y	R_1	R_+	R_-	R_π	Id

where the composition $a \circ b$ is represented by a in the left-most column and b in the top-most row.

Ex. 2.10 For convenience, write $\mathbb{Z}/6\mathbb{Z}$ as $\{0, 1, 2, 3, 4, 5\}$ (instead of using $[\,\cdot\,]_6$ around each number). A subgroup of $\mathbb{Z}/6\mathbb{Z}$ always contains 0, and $\{0\}$ is clearly a subgroup.

If a subgroup contains the element 1, it must also contain $1 + 1 = 2$ and so on, so the only subgroup of $\mathbb{Z}/6\mathbb{Z}$ containing 1 is $\mathbb{Z}/6\mathbb{Z}$ itself. Similarly, if a subgroup contains 5, it must be $\mathbb{Z}/6\mathbb{Z}$.

If a subgroup contains the element 2 or 4, it must also contain $2+2 = 4$ or $4+4 = 2$, respectively, and since $2+4 = 0$, the subset $\{0, 2, 4\}$ is a subgroup.

Since $3 + 3 = 0$, one easily sees that $\{0, 3\}$ is a subgroup of $\mathbb{Z}/6\mathbb{Z}$.

The above mentioned subgroups are the only subgroups of $\mathbb{Z}/6\mathbb{Z}$; which can be seen as follows: Since the order of a subgroup divides the order of the group by Theorem 2.2.8, a subgroup of $\mathbb{Z}/6\mathbb{Z}$ must have either $1, 2, 3$, or 6 elements. Now clearly there is only one subgroup with 1 element, namely $\{0\}$ and only one subgroup with 6 elements, $\mathbb{Z}/6\mathbb{Z}$. If a subgroup has two elements, then the nontrivial element in that group must be its own inverse, and 3 is the only element with this property. If a subgroup has three elements, then the non-trivial elements must be 2 and 4; since clearly none of them can be 5 and 1, and if 3 is in the subgroup then the other nontrivial element must be either 2 or 4; in either case $1 = 3 - 2 = 4 - 3$ is in the subgroup which consequently does not have order 3.

Ex. 2.11 As always, $\{[0]\}$ and $\mathbb{Z}/7\mathbb{Z}$ are clearly subgroups. If $H \subseteq \mathbb{Z}/7\mathbb{Z}$ is a subgroup, then $|H|$ divides $|\mathbb{Z}/7\mathbb{Z}| = 7$ by Theorem 2.2.8, so $|H| = 1$ or $|H| = 7$. In the former case, we must have $H = \{[0]\}$, and in the latter we have $H = \mathbb{Z}/7\mathbb{Z}$.

The same result is clearly true for every prime p; ie. the only subgroups of $\mathbb{Z}/p\mathbb{Z}$ are the trivial ones, $\{[0]\}$ and $\mathbb{Z}/p\mathbb{Z}$.

Ex. 2.12 Let G be a group and H_1, H_2 two proper subgroups of G with the property $H_1 \cup H_2 = G$. Since H_1 is a proper subgroup, we may find an element $x_1 \in G$ which is not in H_1, but since $H_1 \cup H_2 = G$ we must then have $x_1 \in H_2$. Similarly we may find an element x_2 which is not in H_2, but is in H_1. Now $x_1 \circ x_2$ is in at least one of H_1, H_2; assume WLOG $x_1 \circ x_2 \in H_1$. Then since $x_2 \in H_1$ and H_1 is a subgroup, $x_2^{-1} \in H_1$, and then $(x_1 \circ x_2) \circ x_2^{-1} = x_1 \in H_1$, since H_1 is closed under $\circ$. But this contradicts the choice of x_1. In the same way one may show that $x_1 \circ x_2 \notin H_2$, and then $x_1 \circ x_2 \notin H_1 \cup H_2$, and therefore $H_1 \cup H_2 \neq G$.

As an example of a group which is the union of three proper subgroups, consider $G = (\mathbb{Z}/8\mathbb{Z})^*$ and $H_1 = \{[1], [3]\}$, $H_2 = \{[1], [5]\}$, and $H_3 = \{[1], [7]\}$. Then clearly the H_i are subgroups of G, and their union is G.

Ex. 2.13 Let N be a normal subgroup of the group G, ie. $gNg^{-1} = N$ for every $g \in G$. Now let $g \in G$ be given, and consider an element $x \in Ng = \{ng \mid n \in N\}$, so that $x = ng$ for some $n \in n$. Then since $gNg^{-1} = N$ we may find an element $n' \in N$ such that $n = gn'g^{-1}$, from which we see that $x = ng = gn'g^{-1}g = gn' \in gN$. This shows $Ng \subseteq gN$. The other inclusion can be proved in a similar fashion; let $y \in gN$. Then $y = gn$ for some $n \in N$, and using the assumption $N = gNg^{-1}$ for every $g \in G$, it is also true for g^{-1}. This means we may find an element $n' \in N$ such that $n = g^{-1}n'(g^{-1})^{-1} = g^{-1}ng$, but then $y = gg^{-1}ng = ng \in Ng$.

The converse of the above is also true; if $gN = Ng$ for every $g \in G$, then N is normal. For if $n \in N$, is any element, we have $gng^{-1} = (gn)g^{-1} = (n'g)g^{-1} = n' \in N$, so that $gNg^{-1} \subseteq N$. On the other hand, if $n \in N$, then $n = gg^{-1}ngg^{-1} = gg^{-1}(ng)g^{-1} = gg^{-1}(gn')g^{-1} = gn'g^{-1} \in gNg^{-1}$, so that $N \subseteq gNg^{-1}$; ie. N is normal.

Ex. 2.14 Let G be an abelian group and H a subgroup of G. Let g be any element of

G. Then

$$\begin{aligned} gHg^{-1} &= \{ghg^{-1} \mid h \in H\} \\ &= \{gg^{-1}h \mid h \in H\} \\ &= \{h \mid h \in H\} \\ &= H \end{aligned}$$

which shows that H is normal (the abelian property was necessary for the step from the first line to the second).

Ex. 2.15 Let H be a subgroup of the group G.

(i) Since $H = He$, H is a right coset. Now assume $Hg_1 \neq Hg_2$; it is to be shown that their intersection is empty. Assume the existence of an $x \in Hg_1 \cap Hg_2$; then for suitable $h_1, h_2 \in H$ we have $h_1g_1 = h_2g_2$. Since $h_1^{-1}h_2 \in H$, we have $g_1 \in Hg_2$; ie. $g_1 = kg_2$ for some $k \in H$. Now

$$\begin{aligned} Hg_1 &= \{hg_1 \mid h \in H\} \\ &= \{hkg_2 \mid h \in H\} \\ &= \{hk \mid h \in H\}g_2 \\ &= Hg_2 \end{aligned}$$

contrary to the hypothesis (the last step is due to §2.1.6). Thus the assumption $Hg_1 \cap Hg_2 \neq \emptyset$ is false, and distinct right cosets are therefore disjoint.

(ii) Let $\Phi(gH) = Hg^{-1}$. Assume $g_1H = g_2H$. Then by Lemma 2.2.6 $g_1^{-1}g_2 \in H$. But then $(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1 \in H$. Then $g_2^{-1} \in Hg_1^{-1}$, and clearly also $g_2^{-1} \in Hg_2^{-1}$. Thus $Hg_1^{-1} \cap Hg_2^{-1} \neq \emptyset$, and by (i) we must then have $Hg_1^{-1} = Hg_2^{-1}$. Thus Φ is well defined.

To show that Φ is injective, assume $Hg_1^{-1} = Hg_2^{-1}$. Then $Hg_1^{-1}g_2 = H$, and therefore $g_1^{-1}g_2 \in H$. By Lemma 2.2.6 we then have $g_1H = g_2H$; thus Φ is injective.

Let $Hg \in H \setminus G$ be any right coset of H. Then $g^{-1}H \in G/H$ maps to Hg via Φ, so Φ is surjective.

(iii) Assume $|G/H| = 2$. Since Φ (from (ii)) is bijective, we also have $|H \setminus G| = 2$. Thus $H \setminus G = \{H, K\} = G/H$ where $H \cap K = \emptyset$ and $H \cup K = G$. Let $g \in G$ be any element. If $g \in H$ then $gH = H = Hg$ by §2.1.6 and Exercise 2.1. If $g \notin H$ then $g \in K$; then $gH = Hg = K$ since $g \in gH$ and $g \in Hg$. In either case we see that $gH = Hg$. Now from the more general result at the end of Exercise 13, we then see that H is normal. An example of a subgroup of index 3 which is not normal is $\{e, a\} \subseteq S_3$ from Exercise 7.

Ex. 2.16 The composition table looks like this (where $x \circ y$ means multiplying the element x from the leftmost column with y from the top row):

$\circ$	$\mathbf{1}$	$-\mathbf{1}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$\mathbf{1}$	$\mathbf{1}$	$-\mathbf{1}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$-\mathbf{1}$	$-\mathbf{1}$	$\mathbf{1}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{i}$	$-\mathbf{1}$	$\mathbf{1}$	$\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$
$-\mathbf{i}$	$-\mathbf{i}$	$\mathbf{i}$	$\mathbf{1}$	$-\mathbf{1}$	$-\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{1}$	$\mathbf{1}$	$\mathbf{i}$	$-\mathbf{i}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{1}$	$-\mathbf{1}$	$-\mathbf{i}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{1}$	$\mathbf{1}$
$-\mathbf{k}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{1}$	$-\mathbf{1}$

Ex. 2.17 From the composition table above, one easily sees that $\mathbb{H}$ is not abelian, since for instance $\mathbf{ij} = \mathbf{k} \neq -\mathbf{k} = \mathbf{ji}$. From Lagrange's index theorem, a subgroup H of $\mathbb{H}$ has either 1, 2, 4 or 8 elements. The only subgroup containing 1 element is $\{\mathbf{1}\}$, and this is clearly normal. If $|H| = 2$, then H must contain an element apart from $\mathbf{1}$ which is its own inverse, and the only such element is $-\mathbf{1}$; thus the only subgroup with two elements is $\{\mathbf{1}, -\mathbf{1}\}$, and this is also easily seen to be normal (it is well-known from linear algebra that the matrix $-\mathbf{1}$ commutes with every other matrix). If $|H| = 4$, then H has index 2 in $\mathbb{H}$ and by Exercise 2.15 H is normal. Finally the only subgroup of $\mathbb{H}$ with 8 elements is $\mathbb{H}$ itself, which is of course also normal.

Ex. 2.18 Since H and K are subgroups of G, and since K is a subgroup of H, Lagrange's index theorem gives that

$$\begin{aligned} |G| &= |G/H||H| = |G/K||K| \\ |H| &= |H/K||K| \end{aligned}$$

From these equations it is easy to see $|G/H||H/K||K| = |G/K||K|$ and since $|K| \neq 0$ we get $|G/K| = |G/H||H/K|$.

Ex. 2.19 (i) The inverse of $[3]$ in $(\mathbb{Z}/8\mathbb{Z})^*$ is $[3]$, since $[1]$ is the neutral element and $[3]^2 = [3^2] = [9] = [1]$. Actually $x^{-1} = x$ for all $x \in (\mathbb{Z}/8\mathbb{Z})^*$.

(ii) The inverse of $[5]$ in $(\mathbb{Z}/13\mathbb{Z})^*$ is $[8]$ because $[5][8] = [40] = [1]$.

Ex. 2.20 Let $f\colon G \xrightarrow{\sim} H$ be a group isomorphism, and let $f^{-1}\colon H \to G$ denote its inverse. Let $x, y \in H$. Then $x = f(a)$ for a uniquely determined $a \in G$, since f is bijective; likewise $y = f(b)$. Then $f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y)$, which shows that f^{-1} is a group homomorphism (and therefore also a group isomorphism).

Ex. 2.21 Let G be a group with composition $\circ$ and define $f\colon G \to G$ by $f(g) = g^2 = g \circ g$. If f is a group homomorphism, then for any $x, y \in G$ we have $(xy) \circ (xy) = f(xy) = f(x)f(y) = x^2y^2$. Multiplying from the left with x^{-1} and from the right with y^{-1} and using that $\circ$ is associative, one sees that for any $x, y \in G$ we have $yx = xy$, thus G is abelian.

Conversely, if G is abelian, $yx = xy$ for all $x, y \in G$. Multiplying with x and y from the left and right, respectively, one sees that $xyxy = x^2y^2$, proving that f is in fact a group homomorphism.

Ex. 2.22 Let $\xi\colon \mathbb{R} \to \mathbb{R}_{>0}$ denote the exponential function $x \mapsto e^x$. Considering $\mathbb{R}$ as an additive group and $\mathbb{R}_{>0}$ as a multiplicative group, we see that $\xi(x+y) = e^{x+y} = e^x e^y = \xi(x)\xi(y)$; thus ξ is a group homomorphism. It is bijective because the exponential function is strictly increasing and its range is exactly $\mathbb{R}_{>0}$. The inverse is the natural logarithm $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$ (reflecting the well-known property $\log(xy) = \log(x) + \log(y)$).

Ex. 2.23 Define $\operatorname{sgn}\colon S_3 \to \mathbb{Z}/2\mathbb{Z}$ by $e, d, f \mapsto [0]$ and $a, b, c \mapsto [1]$. Then using the composition table from Example 2.1.6, one may verify that $\operatorname{sgn}(x \circ y) = \operatorname{sgn}(x) + \operatorname{sgn}(y)$ for every pair of elements $x, y \in S_3$, so that sgn is in fact a group homomorphism $S_3 \to \mathbb{Z}/2\mathbb{Z}$.

Ex. 2.24 Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then one may easily by induction show that

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Thus for all $n \in \mathbb{N} \setminus \{0\}$ we have $A^n \neq I$, which means that A has infinite order.

Ex. 2.25 A (real) vector space V is closed under addition, has a neutral element 0 and every vector v has an additive inverse $-v$; thus V is seen to be an additive group. Another characteristic of a vector space is that $+$ is commutative, meaning that V regarded as an additive group is abelian. A subspace W of V may also be considered as an additive group, and is therefore a subgroup of V; it is normal because V is abelian (making all subgroups normal, cf. Exercise 2.14). The quotient group V/W is clearly an abelian additive group. It remains to show that the scalar multiplication given by $\lambda(v+W) = \lambda v+W$ is well defined. Suppose $v_1 + W = v_2 + W$. This means $v_1 - v_2 \in W$, and so $\lambda(v_1 - v_2) = \lambda v_1 - \lambda v_2 \in W$. Consequently $\lambda v_1 + W = \lambda v_2 + W$, and the scalar multiplication is well defined.

Ex. 2.26 Clearly $f(G) = H$ is a subgroup of K; if $a, b \in H$ then $a = f(x)$, $b = f(y)$, and $ab = f(x)f(y) = f(xy) \in f(G)$, $e = f(e) \in H$ and $f(e) = f(xx^{-1}) = f(x)f(x^{-1}) = af(x^{-1}) = e$, so that $a^{-1} = f(x^{-1}) \in f(G)$. H is abelian because $ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba$.

Ex. 2.27 Let $A \in \mathrm{GL}_2(\mathbb{R})$ and $B \in \mathrm{SL}_2(\mathbb{R})$. Then

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = 1,$$

such that $ABA^{-1} \in \mathrm{SL}_2(\mathbb{R})$. Thus for any $A \in \mathrm{GL}_2(\mathbb{R})$ we have

$$A\,\mathrm{SL}_2(\mathbb{R})A^{-1} \subseteq \mathrm{SL}_2(\mathbb{R}). \tag{2.2}$$

Now this is actually enough to conclude that $\mathrm{SL}_2(\mathbb{R})$ is normal; ie. the inclusion (2.2) implies the opposite inclusion, which one may show in full generality:

Let G be a group and H a subgroup of G which satisfies

$$\forall g \in G\colon gHg^{-1} \subseteq H \tag{2.3}$$

We wish to show that for all elements $g \in G$ the other inclusion is true. Now let $g \in G$ and $h \in H$ be given. Since the assumption (2.3) is true for all g, it also holds for g^{-1}. Thus we have $g^{-1}hg = k \in H$. Then $h = gkg^{-1} \in gHg^{-1}$. Thus $H \subseteq gHg^{-1}$ as required.

The determinant $\det\colon \mathrm{GL}_2 \to \mathbb{R}\setminus\{0\}$ is clearly a group homomorphism (Example 2.4.3). It is surjective, since $\det\begin{pmatrix} x & 0 \\ 0 & 1\end{pmatrix} = x$. Now since the neutral element in $(\mathbb{R}\setminus\{0\}, \cdot)$ is 1, the kernel for det is exactly $\mathrm{SL}_2(\mathbb{R})$. Thus the isomorphism theorem states that $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R})$ is isomorphic to the multiplicative group $(\mathbb{R}\setminus\{0\}, \cdot)$.

Since $\mathrm{SL}_2(\mathbb{R})$ is the kernel of det, the normality of $\mathrm{SL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$ may also be seen directly from Proposition 2.4.9.

Ex. 2.28 A generator for $(\mathbb{Z}/13\mathbb{Z})^*$ is $[2]$, which can be seen by explicitly computing $\langle[2]\rangle$:

$$\begin{aligned}\langle[2]\rangle &= \{[2],[4],[8],[3],[6],[12],[11],[9],[5],[10],[7],[1]\}\\ &= (\mathbb{Z}/13\mathbb{Z})^*.\end{aligned}$$

Ex. 2.29 Consider the group $G = (\mathbb{Z}/q\mathbb{Z})^*$. Since q divides 2^p-1, $2^p \equiv 1 \pmod{q}$, and thus $[2]^p = [1]$ in G. It then follows from Proposition 2.6.3 that $\operatorname{ord}([2]) \mid p$. But $\operatorname{ord}([2]) \neq 1$ since $[2] \neq [1]$, and then since p is a prime, $\operatorname{ord}([2]) = p$. The order of an element divides the order of the group, and since q is a prime $|G| = \varphi(q) = q-1$. Thus p divides $q-1$, and this is only possible if $q > p$.

Now assume there is only a finite number of primes. Then choose the largest among these, say P. Then choose a prime factor of 2^P-1; this prime factor is larger than P by the above, and thus larger than all primes, which is a contradiction. Thus there must be infinitely many primes.

Ex. 2.30 Let $\pi\colon G \to G/N$ denote the canonical group homomorphism, where N is a normal subgroup of the group G.

(i) Let K be a subgroup of G. Then for any two elements $a,b \in \pi(K)$ we have $a = xN = \pi(x)$ and $b = yN = \pi(y)$ for some $x,y \in K$. Now this means $ab = (xN)(yN) = \pi(x)\pi(y) = \pi(xy) = xyN \in \pi(K)$, since $xy \in K$. Clearly $N = eN \in \pi(K)$, and the inverse of a is $a^{-1} = x^{-1}N = \pi(x^{-1})$; since K is a group $x^{-1} \in K$ so that $a^{-1} \in \pi(K)$.

(ii) Let H be a subgroup of G/N. Since N is the neutral element in H, and since $nN = N$ for every $n \in N$, we clearly have $N \subseteq \pi^{-1}(H)$. If x,y are elements of $\pi^{-1}(H)$ then $\pi(x),\pi(y) \in H$; thus $\pi(x)\pi(y) = \pi(xy) \in H$ so that $xy \in \pi^{-1}(H)$. Since $e \in N$ and $N \subseteq \pi^{-1}(H)$ we have $e \in \pi^{-1}(H)$. Finally, since $\pi(x^{-1})$ is the inverse element of $\pi(x)$ in H, $\pi(x^{-1}) \in H$ and $x^{-1} \in \pi^{-1}(H)$.

(iii) The inclusion $\pi(\pi^{-1}(H)) \subseteq H$ is true for any map $\pi\colon X \to Y$ and any subset $H \subseteq Y$. So assume $h \in H$. Then $h = xN$ for some $x \in G$; we have $x \in \pi^{-1}(H)$, which again implies $\pi(x) = h \in \pi(\pi^{-1}(H))$, so $H \subseteq \pi(\pi^{-1}(H))$, hence the desired equality.

As above, one may argue that for any map $\pi\colon X \to Y$ and any subset $K \subseteq X$ we have $K \subseteq \pi^{-1}(\pi(K))$. Now assume $K \supseteq N$ is a subgroup of G containing N. Let $x \in \pi^{-1}(\pi(K))$. Then by definition $\pi(x) \in \pi(K)$, but this means that there exists $k \in K$ such that $\pi(x) = xN = \pi(k) = kN$. Then by Lemma 2.2.6 we have $k^{-1}x \in N$. Since N is a subgroup of K, this means $x = k(k^{-1}x) \in K$, so that $\pi^{-1}(\pi(K)) \subseteq K$.

(iv) Let G be a cyclic group, and let $a \in G$ be a generator for G. If $f\colon G \to K$ is a surjective group homomorphism, then $f(a)$ is a generator for K; because if k is some element in K, then $k = f(x)$ for some $x \in G$. Since a generates G, we have $x = a^n$ for some $n \in \mathbb{Z}$; thus $k = f(x) = f(a^n) = f(a)^n$.

(v) If H is a subgroup of $\mathbb{Z}/N\mathbb{Z}$, then by (ii) we have that $\pi^{-1}(H)$ is a subgroup of $\mathbb{Z}$, which is cyclic by Proposition 2.2.3. Since $\pi(\pi^{-1}(H)) = H$, we see that $\pi_{|\pi^{-1}(H)}\colon \pi^{-1}(H) \to H$ is a surjective group homomorphism; thus by (iv) we may conclude that H is cyclic.

Ex. 2.31 (i) From Proposition 2.7.4 we know that there are exactly $\varphi(7) = 6$ elements of order 7 in $\mathbb{Z}/28\mathbb{Z}$; and these are the generators of the unique subgroup of order 7. Since $[4]^7 = [28] = [0]$, $\operatorname{ord}([4])$ divides 7, and since 7 is a prime then $\operatorname{ord}([4]) = 7$. Thus all elements of order 7 are the nontrivial elements of $\langle [4] \rangle$; ie.

$$[4], [8], [12], [16], [20], [24]$$

(ii) As mentioned above there is exactly one subgroup of order 7.

Ex. 2.32 (i) Since 3 and 5 are relatively prime integers, it follows directly from the Chinese Remainder Theorem (Proposition 2.8.2) that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$.

(ii) Since $(\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$, the product group $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (because if $\varphi_1\colon G_1 \to H_1$ and $\varphi_2\colon G_2 \to H_2$ are group isomorphisms, then the map

$$\varphi\colon G_1 \times G_2 \to H_1 \times H_2$$

defined by $\varphi(x, y) = (\varphi_1(x), \varphi_2(y))$ is a group isomorphism).

Now let $\varphi\colon \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ be the isomorphism defined in Proposition 2.8.2 (ie. $\varphi([x]_{15}) = ([x]_3, [x]_5)$), and consider the restriction $f = \varphi|_{(\mathbb{Z}/15\mathbb{Z})^*}\colon (\mathbb{Z}/15\mathbb{Z})^* \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Since representatives of elements in $(\mathbb{Z}/15\mathbb{Z})^*$ are relatively prime to 15, they are also relatively prime to 3 and 5; thus not divisible by 3 nor 5, and we may consider f as a map into $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$. Now since φ is injective, clearly also f is injective. f is then also surjective, because $|(\mathbb{Z}/15\mathbb{Z})^*| = 8 = 2 \cdot 4 = |(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*|$. It remains to show that

f is in fact a group homomorphism:

$$\begin{aligned} f([x]_{15}[y]_{15}) &= f([xy]_{15}) \\ &= ([xy]_3, [xy]_5) \\ &= ([x]_3[y]_3, [x]_5[y]_5) \\ &= ([x]_3, [x]_5)([y]_3, [y]_5) \\ &= f([x]_{15})f([y]_{15}) \end{aligned}$$

Since the order of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is 8, and the maximum order of an element is 4, the group cannot be cyclic. Thus $(\mathbb{Z}/15\mathbb{Z})^*$ is not cyclic.

Ex. 2.33 (i) Let $g = \left[\frac{9}{4}\right] \in \mathbb{Q}/\mathbb{Z}$. The neutral element in $\mathbb{Q}/\mathbb{Z}$ is $[0] = 0 + \mathbb{Z} = \mathbb{Z}$. Then $g = \left[\frac{9}{4} - 2\right] = \left[\frac{1}{4}\right]$, and the order of g is then seen to be 4, since 4 is the smallest number for which $g^n = [0]$.

(ii) Since $\mathbb{Q}/\mathbb{Z}$ is an additive group, $\left[\frac{a}{b}\right]^n = \left[n\frac{a}{b}\right]$. The order of $\left[\frac{a}{b}\right]$ is the smallest positive integer for which $\left[n\frac{a}{b}\right] = [0]$, ie. the smallest n for which $\frac{na}{b}$ is an integer. Now since $\gcd(a, b) = 1$, b divides na if and only if b divides n. The smallest n for which this occurs is $n = b$. Thus $\operatorname{ord}\left(\left[\frac{a}{b}\right]\right) = b$. Since every rational number has a (unique) representation as an irreducible fraction with positive denominator, and elements of $\mathbb{Q}/\mathbb{Z}$ are of the form $q + \mathbb{Z}$, where q is a rational number, all elements of $\mathbb{Q}/\mathbb{Z}$ have finite order. Since $\gcd(1, n) = 1$ for all $n \geq 1$, the element $\left[\frac{1}{n}\right]$ has order n, and thus we may find elements of $\mathbb{Q}/\mathbb{Z}$ with arbitrary large order.

(iii) Assuming $\mathbb{Q}/\mathbb{Z}$ is finite, let $\mathbb{Q}/\mathbb{Z} = \{a_1, a_2, \ldots, a_N\}$. Now let $m_i = \operatorname{ord}(a_i)$ and let M be the largest of the m_i. Since we may find elements of arbitrary large order in $\mathbb{Q}/\mathbb{Z}$, we may find an element x with $\operatorname{ord}(x) > M$. But this contradicts M being the largest of the orders of the elements of $\mathbb{Q}/\mathbb{Z}$; thus the quotient group cannot be finite. If $\mathbb{Q}/\mathbb{Z}$ is generated by g, then $\operatorname{ord}(g) = |\langle g\rangle|$ is infinite; but from (ii) every element has finite order, which is a contradiction. Thus $\mathbb{Q}/\mathbb{Z}$ cannot be cyclic.

Ex. 2.34 Assume $G = (\mathbb{Q} \setminus \{0\}, \cdot)$ is generated by $\frac{a}{b}$. We may WLOG assume that $b > 0$ and $\gcd(a, b) = 1$. Now since $\frac{a}{b}$ generates $(\mathbb{Q} \setminus \{0\}, \cdot)$ we may find an $n \in \mathbb{Z}$ such that $\frac{a^n}{b^n} = -1$. From this we see that a must be negative (and that n is odd). Thus $(-a)^n = b^n$, and since $-a$ and b are positive numbers $-a = b$. But $\gcd(a, b) = \gcd(-a, b) = \gcd(b, b) = 1$, meaning that $-a = b = 1$; thus $\frac{a}{b} = -1$. But $\langle -1\rangle = \{-1, 1\} \subsetneq \mathbb{Q} \setminus \{0\}$, which contradicts the assumption.

Another way to see this is to observe that group isomorphisms preserve the order of elements. If G is cyclic, it must be isomorphic to $\mathbb{Z}$ (since the latter is "the only" infinite cyclic group). Since $\operatorname{ord}_G(-1) = 2$ in G, we see that $\mathbb{Z}$ contains an element of order 2, which is false.

Yet another argument is this: If $(\mathbb{Q} \setminus \{0\}, \cdot)$ is cyclic, so is the subgroup $(\mathbb{Q}_{>0}, \cdot)$. We may WLOG assume that the generator $x = \frac{a}{b} > 1$, since x and x^{-1} generate the same group. But since we may find a rational number y such that $1 < y < x$, and since clearly $x^n \neq y$ for all $n \in \mathbb{Z}$, we see that $\langle x \rangle \subsetneq \mathbb{Q}_{>0}$.

Ex. 2.35 A non-cyclic group of order 8 may be constructed as $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, since every element in this product group other than $([0], [0], [0])$ has order 2. Another example is the quaternion group from Exercises 16–17; it is clearly not cyclic since it is not abelian. Yet another example is the group $(\mathbb{Z}/15\mathbb{Z})^*$ from Exercise 32.

Ex. 2.36 Let G be a finite group of order N. Let $\psi(d)$ denote the number of elements in G of order d.

(i) Since the order of an element divides the order of the group (Proposition 2.6.3), no element has order d if $d \nmid N$; thus $\psi(d) = 0$ for $d \nmid N$. If $\psi(N) > 0$ there is at least one element $g \in G$ such that $\operatorname{ord}(g) = |G| = N$; thus the subgroup generated by g is G; so G is cyclic. If on the other hand G is cyclic, G is generated by some element, say g. Then $\operatorname{ord}(g) = N$ and $\psi(N) \geq 1 > 0$.

(ii) Since every element in G has a unique order d, which is a divisor of N, we see that we may count the elements of G by the formula

$$N = \sum_{d \mid N} \psi(d).$$

(iii) Now assume that for every divisor d in N, G contains a unique subgroup of order d.

If $d \nmid N$ then $\psi(d) = 0 \leq \varphi(d)$ trivially. If $d \mid N$, let H denote the unique subgroup of order d. Assume $\psi(d) > \varphi(d)$. For each of the elements $g_1, \dots, g_{\psi(d)}$ of order d, consider the cyclic subgroup $H_i = \langle g_i \rangle$. All of these groups has order d; thus $H_i = H$ for all i. But then H is certainly cyclic, and has exactly $\varphi(d)$ generators by Proposition 2.7.4 (notice that it is *not* assumed that the "parent group" G is cyclic; we simply consider H as a group in itself, and uses the proposition for

$H \subseteq H$ and $d = |H|$). But since all of the g_i generates H, and there are $\psi(d)$ such g_i, the original assumption that $\psi(d) > \varphi(d)$ must be false.

Now the inequality $\psi(d) \leq \varphi(d)$ and the equations

$$N = \sum_{d|N} \psi(d) = \sum_{d|N} \varphi(d)$$

implies that $\psi(d) = \varphi(d)$ for all $d \mid N$ (since if there were a d where strict inequality was the case, we would also have a strict inequality in the above equations). Thus in particular $\psi(N) = \varphi(N) > 0$, so G is cyclic by (i).

Ex. 2.37 Since the sign of a transposition is -1, the sign of a product of an odd number n of transpositions is $(-1)^n = -1$; thus an even permutation (which has sign $+1$) is not the product of an odd number of transpositions.

Ex. 2.38 Let $\sigma = (i_1 \cdots i_k)$ be a k-cycle in S_n. Then $\sigma^r(i_1) = i_{r+1}$ for $1 \leq r < k$, so that $\sigma^r \neq \mathrm{Id}$. For $r = k$ we see that every element i_j is "moved" exactly k times to the right, so that $\sigma^k = \mathrm{Id}$. Thus $\mathrm{ord}(\sigma) = k$.

Ex. 2.39 Since $\langle\tau\rangle = \{(123), (213), (1)(2)(3)\}$, $|\langle\tau\rangle| = 3$, so $[S_3 : \langle\tau\rangle] = 2$; thus by Exercise 15(iii) $\langle\tau\rangle$ is normal in S_3.

Ex. 2.40 (i) According to Proposition 2.9.17, the sign of a 5-cycle is $(-1)^{5-1} = 1$, so (12345) is even. The order of $\langle\sigma\rangle$ may be found be explicitly calculating σ^n for $n = 1, 2, \ldots$. This gives

$$\begin{aligned}
\sigma &= (12345)\\
\sigma^2 &= (13524)\\
\sigma^3 &= (14253)\\
\sigma^4 &= (15432)\\
\sigma^5 &= (1)(2)(3)(4)(5) = \mathrm{Id},
\end{aligned}$$

which shows that $|\langle\sigma\rangle| = 5$.

(ii) Let $\tau = (12)$. Then from Lemma 2.9.8 we see that $\tau\sigma\tau^{-1} = (21345) \notin \langle\sigma\rangle$; thus $\langle\sigma\rangle$ is not normal.

Ex. 2.41 (i) Since $\mathrm{sgn}\colon S_n \to (\{\pm 1\}, \cdot)$ is a group homomorphism, and since $(\{\pm 1\}, \cdot)$ is abelian, we see that

$$\begin{aligned}
\mathrm{sgn}(\tau\sigma\tau^{-1}) &= \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau^{-1})\\
&= \mathrm{sgn}(\tau)\,\mathrm{sgn}(\tau^{-1})\,\mathrm{sgn}(\sigma)\\
&= \mathrm{sgn}(\tau\tau^{-1})\,\mathrm{sgn}(\sigma)\\
&= \mathrm{sgn}(\sigma)
\end{aligned}$$

(ii) It is easy to see that $(123) = (12)(23)$. If $\sigma = (abc)$ is any 3-cycle, let $\tau \in S_4$ be the permutation defined by $\tau(a) = 1$, $\tau(b) = 2$, and $\tau(c) = 3$. Then by Lemma 2.9.8 we have $\tau\sigma\tau^{-1} = (\tau(a)\,\tau(b)\,\tau(c)) = (123)$. Then for any 3-cycle σ we have $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau\sigma\tau^{-1}) = \operatorname{sgn}((123))$. By writing

$$(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

it is easy to see that $I_{(123)} = \{(1,3),(2,3)\}$ and $n((123)) = |I_{(123)}| = 2$ (Definition 2.9.10); then $\operatorname{sgn}(123) = (-1)^2 = 1$; thus all 3-cycles are even (and therefore belong to A_4). If $\sigma = (abc)$, then $\sigma^2 = (acb)$ and $\sigma^3 = (a)(b)(c) = \mathrm{Id}$, so the order of any 3-cycle in A_4 is 3.

(iii) A 3-cycle is determined the element which is not "moved" by the permutation, and the way the other three elements are permuted (there are two possibilities; one of the elements must be mapped to one of the other two; once this choice has been made the 3-cycle is determined). This gives in all 8 different 3-cycles in A_4. If H is any subgroup of A_4 which contains all 3-cycles, $|H| \geq 8$, and since the order of a subgroup divides the order of the group, and since $|A_4| = 12$, we must have $|H| = 12$ which means $H = A_4$.

(iv) If $\varphi\colon A_4 \to \mathbb{Z}/2\mathbb{Z}$ is a group homomorphism, then $\varphi(\mathrm{Id}) = [0]$. For any 3-cycle $\sigma \in A_4$ we have $\varphi(\sigma)^3 = \varphi(\sigma^3) = \varphi(\mathrm{Id}) = [0]$, and this necessarily means $\varphi(\sigma) = [0]$ (since $[1]^3 = [1]$). Since the kernel of a group homomorphism is a subgroup of the homomorphism domain, $\operatorname{Ker}\varphi \subseteq A_4$, and since all 3-cycles are in $\operatorname{Ker}\varphi$, we must have (from (iii)) that $\operatorname{Ker}\varphi = A_4$; thus $\varphi(\sigma) = [0]$ for all $\sigma \in A_4$.

(v) Assume A_4 contains a subgroup H of order 6. Then $[A_4 : H] = 2$ and H is normal. Then A_4/H is a group with 2 elements, say $\{[\mathrm{Id}], [\sigma]\}$. It is clearly (group) isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (as are all groups with two elements). Let $\tilde{f}$ be an isomorphism ($\tilde{f}([\mathrm{Id}]) = [0]$ and $\tilde{f}([\sigma]) = [1]$). Let $\pi\colon A_4 \to A_4/H$ denote the canonical homomorphism. Since composition of homomorphisms gives a homomorphism, $\tilde{f} \circ \pi$ is a homomorphism from A_4 to $\mathbb{Z}/2\mathbb{Z}$. Now $\tilde{f}\circ\pi(\sigma) = \tilde{f}([\sigma]) = [1]$, which contradicts (iv). Thus there cannot be a subgroup of A_4 of order 6.

Ex. 2.42 The cases $n = 1$ and $n = 2$ are trivial, since $|A_1| = |A_2| = 1$, so clearly there can be no subgroup of index 2. Let $n \geq 3$, and assume g is a group homomorphism from A_n to $\mathbb{Z}/2\mathbb{Z}$. Let σ be a 3-cycle in A_n. Then as above we see that $[0] = g(\mathrm{Id}) = g(\sigma^3) = g(\sigma)^3$ such that $g(\sigma) = [0]$. But by Lemma 2.9.18 we may write every permutation in A_n as a product of 3-cycles, so this implies that $g(\sigma) = [0]$ for every $\sigma \in A_n$. Now assume H is a subgroup of A_n of index 2. Then H is normal, and A_n/H is a group which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Thus we have a surjective group homomorphism $\pi\colon A_n \to A_n/H$ and a group isomorphism $\tilde{f}\colon A_n/H \to \mathbb{Z}/2\mathbb{Z}$. Then the composition $g = \tilde{f} \circ \pi$ is a group homomorphism from A_n to $\mathbb{Z}/2\mathbb{Z}$. It is surjective because π and $\tilde{f}$ are surjective (see Figure 1). But this contradicts that $g(\sigma) = [0]$ for every σ, so no such H can exist.

$$\begin{tikzcd}
A_n \arrow[rr, two heads, "\pi"] \arrow[dr, two heads, "\tilde{f}\circ\pi"'] & & A_n/H \arrow[dl, hook, two heads, "\tilde{f}"] \\
& \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

Figure 1: A diagram showing that $\tilde{f} \circ \pi$ is surjective

Ex. 2.43 From §2.9.2 we have that

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \\ &= (65)(54)(65)(43)(54)(65)(32)(43)(54)(65)(21)(32)(43)(54)(65)\end{aligned}$$

ie. that σ is the product of 15 simple transpositions. Since $n(\sigma) = 15$, this is the least possible number by Proposition 2.9.14.

Ex. 2.44 An element σ of order 2 in A_6 is a permutation of the form $(ij)(kl)$ where i, j, k, l are distinct numbers among $\{1, 2, 3, 4, 5, 6\} = M_6$. This may be seen as follows: Since the order is 2, σ is not the identity. Thus there is a least element $i \in M_6$ such that $\sigma(i) = j \neq i$. Now writing σ as a product of disjoint cycles, we see that σ contains the 2-cycle (ij); if j did not map to i under σ, then the order of σ would not be 2. Now since σ is even, there must be another such 2-cycle, disjoint from (ij), say (kl). This clearly determines σ completely. Conversely, every permutation of the form $(ij)(kl)$ is an even permutation of order 2.

Counting the number of elements of order 2 in A_6 is now easy: There are $\binom{6}{4} = 15$ ways of choosing 4 numbers from M_6. From these numbers, it is possible to construct 3 different permutations, namely $(ij)(kl)$, $(ik)(jl)$, and $(il)(jk)$ (fixing the i we can choose three different neighbors for i, putting the remaining numbers in the other cycle). Thus there are $15 \cdot 3 = 45$ elements of order 2 in A_6.

Ex. 2.45 Since the order of A_3 is $3!/2 = 3$, the only subgroups of A_3 are the trivial ones A_3 and $\{e\}$, so A_3 is simple.

Let H denote the subgroup formed by the elements of order 2 and the neutral element of A_4. This is a group of order 4. The elements are Id, (12)(34), (13)(24), and (14)(23). Now let $\sigma \in A_4$. Then $\sigma H \sigma^{-1}$ is the set

$$\{\mathrm{Id}, (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)), (\sigma(1)\sigma(3))(\sigma(2)\sigma(4)), (\sigma(1)\sigma(4))(\sigma(2)\sigma(3))\}$$

by Lemma 2.9.8. A little thought reveals that this set is in fact H itself (the non-trivial elements all have order 2, and there are exactly 3 such elements in A_4). Thus H is a non-trivial normal subgroup in A_4, which is therefore not simple.

Ex. 2.46 The rotations and reflections which map K to itself are $G = \{I, R, S, T, D, E\}$, where I is the identity map, D, E are rotations with $2\pi/3$ and $4\pi/3$, respectively, around the center of K, and R, S, T are reflections in the medians of K. Using k colors, we may color K in k^3 different ways which are preserved under I. If we rotate K, we may freely choose the color for one side, ie. k different colorings, but then the colors of the remaining sides must be the same color. If we reflect K in a line through the center and a vertex, the side opposite the vertex is mapped to itself, and thus may be freely colored. The two sides joined at the vertex are mapped to each other and must therefore be colored alike. Thus there are k^2 colorings of K which are preserved under a reflection. From Burnside's lemma we now see that the number of different colorings, taking two colorings two be equal if one can be rotated and/or reflected into the other, is

$$\frac{\sum_{g \in G} |S^g|}{|G|} = \frac{k^3 + 3k^2 + 2k}{6}$$

where S is the total set of colorings.

Ex. 2.47 (i) A representative for each of the 8 orbits can be seen in figure 2.

(ii) If only rotations are taken into account, there are 10 essentially different colorings of O. In addition to those shown in figure 2, the colorings in figure 3 are representatives of these colorings.

(iii) By comparing figures 2 and 3, we see that the colorings invariant under rotations but not under reflections are exactly the colorings which are not symmetric with respect to any axis; ie. the colorings x for which the stabilizer G_x does not contain any reflections.

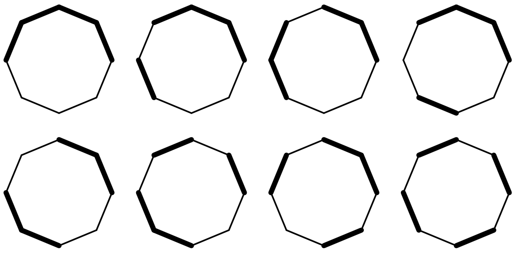

Figure 2: The 8 essentially different colorings of the octagon O

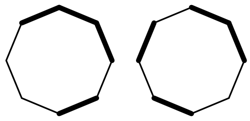

Figure 3: The two additional colorings

Ex. 2.48 There are $\binom{16}{8} = 12870$ different ways of coloring a 4×4 board when half of the squares must be white and the other half black. There are 4 rotations and 4 reflections of the plane which maps the board to itself, namely:

(I) The identity Id (a rotation of 0).

(II) Rotations of $\pm\pi/4$ around the center.

(III) A rotation of $\pi/2$ around the center.

(IV) Two reflections in the axes parallel to the board's sides.

(V) Two reflections in the diagonals of the board.

Observe that these are exactly the rotations and reflections from Exercise 2.9. Now the number of colorings invariant under each of these types of transformations are

(I) 12870.

(II) 6, since 2 squares in each of the quadrants must be colored white (and the other 2 black), and there are $\binom{4}{2} = 6$ ways of doing this.

(III) 70, since 4 squares in the upper half plane must be colored white; this can be done in $\binom{8}{4} = 70$ ways.

(IV) 70, for the same reason as above.

(V) 150, but this one is a bit tricky: First observe that the squares along the diagonal are mapped to themselves. There must be an even number $(0, 2$ or $4)$ squares on the diagonal which are colored white, since otherwise there would be an odd number of white squares above the diagonal and an even number of white squares below the diagonal (or vice versa). First consider the case where all 4 diagonal squares are colored white. Then 2 squares below the diagonal must be white as well (and this completely determines the coloring); this can be done in $\binom{6}{2} = 15$ ways. By symmetry, there are also 15 colorings where the diagonal is entirely black. The last possibility is that 2 diagonal squares are white and the other 2 black; and for each way of coloring the diagonal in this way, 3 squares below the diagonal must be colored white. This gives yet another $\binom{4}{2}\binom{6}{3} = 120$ different colorings; thus in all 150.

With the above numbers, it is easy to calculate the number of essentially different colorings; Burnside's lemma gives

$$\sum_{g\in G} \frac{|S^g|}{|G|} = \frac{12870 + 2\cdot 6 + 70 + 2\cdot 70 + 2\cdot 150}{8} = 1674.$$

Ex. 2.49 Let $\sigma_1 = (1)(2)(345)$, $\sigma_2 = (3)(4)(152)$, and $\tau = (13)(245)$.

(i) Writing τ as

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

we see that $n(\tau) = 5$. Thus according to Proposition 2.9.14 we may write τ as a product of 5 simple transpositions, which is the least possible number.

(ii) Since $\mathrm{sgn}(\tau) = (-1)^{n(\tau)} = -1$, τ is odd and thus does not belong to A_5. Using Lemma 2.9.8 we find

$$\begin{aligned} \tau\sigma_1\tau^{-1} &= (\tau(1))(\tau(2))(\tau(3)\,\tau(4)\,\tau(5)) \\ &= (3)(4)(152) \\ &= \sigma_2 \end{aligned}$$

(iii) Since both σ_1 and σ_2 are 3-cycles, their sign is $(-1)^{3-1} = 1$ (Proposition 2.9.17); thus they are even and belong to A_5. Since sgn is a group homomorphism, $\operatorname{sgn}(\tau_1) = \operatorname{sgn}((34)\tau) = \operatorname{sgn}((34))\operatorname{sgn}(\tau) = (-1)^2 = 1$; thus $\tau_1 \in A_5$. Finally, again using Lemma 2.9.8 we see

$$\begin{aligned}\tau_1\sigma_1\tau_1^{-1} &= (\tau_1(1))(\tau_1(2))(\tau_1(3)\,\tau_1(4)\,\tau_1(5))\\ &= (4)(3)(152)\\ &= \sigma_2\end{aligned}$$

(since (4) and (3) are disjoint and therefore commute).

(iv) (a) The only permutation of cycle type $1 \leq 1 \leq 1 \leq 1 \leq 1$ is the identity, which is clearly even ($n(\mathrm{Id}) = 0$).

(b) Using Proposition 2.9.17 we find the sign of a permutation of cycle type $1 \leq 2 \leq 2$ to be $(-1)^{1-1}(-1)^{2-1}(-1)^{2-1} = 1$.

(c) Likewise the sign of a permutation of cycle type $1 \leq 1 \leq 3$ is $(-1)^{1-1}(-1)^{1-1}(-1)^{3-1} = 1$

(d) Finally the sign of a 5-cycle is $(-1)^{5-1} = 1$.

As already mentioned, the only permutation of the cycle type in (a) above is the identity, which is conjugate to itself via any permutation in A_5.

If σ_1 and σ_2 have the cycle type $1 \leq 2 \leq 2$, then we know they are conjugate via the permutation $\tau \in S_5$. If $\tau \in A_5$, we are done. If not, choose one of the 2-cycles of σ_1 (call it $(\alpha\beta)$), and define $\tau' = \tau(\alpha\beta)$. Then clearly τ' is even. It then follows that σ_1 and σ_2 are conjugate via τ', since

$$\begin{aligned}\tau'\sigma_1\tau'^{-1} &= \tau(\alpha\beta)(\alpha\beta)(\gamma\delta)(\varepsilon)[(\alpha\beta)^{-1}\tau^{-1}]\\ &= \tau(\gamma\delta)(\varepsilon)(\alpha\beta)\tau^{-1}\\ &= \tau\sigma_1\tau^{-1}\\ &= \sigma_2\end{aligned}$$

since a 2-cycle is its own inverse and disjoint cycles commute.

Now let σ_1, σ_2 be of the cycle type in (c) above; again they are conjugate via the permutation $\tau \in S_5$. If $\tau \in A_5$ we are done. If not, write σ_1 as $(\alpha)(\beta)(\gamma\delta\varepsilon)$ and let $\tau' = \tau(\alpha\beta)$. Again, τ' is even, and

$$\begin{aligned}\tau'\sigma_1\tau'^{-1} &= \tau(\alpha\beta)(\alpha)(\beta)(\gamma\delta\varepsilon)[(\alpha\beta)^{-1}\tau^{-1}]\\ &= \tau(\alpha\beta)(\gamma\delta\varepsilon)(\alpha\beta)\tau^{-1}\\ &= \tau(\gamma\delta\varepsilon)\tau^{-1}\\ &= \sigma_2\end{aligned}$$

since $(\alpha\beta)$ commutes with $(\gamma\delta\varepsilon)$. Thus σ_1 and σ_2 are conjugate via a permutation in A_5.

(v) Let $\sigma_1 = (12345)$ and $\sigma(2) = (21345)$. Then if σ_1 and σ_2 are conjugate via $\tau \in A_5$, we have

$$\begin{aligned}&\tau\sigma_1\tau^{-1} = \sigma_2 \Longrightarrow\\ &(\tau(1)\,\tau(2)\,\tau(3)\,\tau(4)\,\tau(5)) = (21345)\end{aligned}$$

τ is then uniquely determined once $\tau(1)$ is specified. For each possibility we now find $n(\tau)$:

$$\begin{aligned}
\tau(1) = 1 \quad &\Rightarrow \quad \tau = \begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix} \quad \Rightarrow \quad n(\tau) = 3\\
\tau(1) = 2 \quad &\Rightarrow \quad \tau = \begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix} \quad \Rightarrow \quad n(\tau) = 1\\
\tau(1) = 3 \quad &\Rightarrow \quad \tau = \begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix} \quad \Rightarrow \quad n(\tau) = 7\\
\tau(1) = 4 \quad &\Rightarrow \quad \tau = \begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix} \quad \Rightarrow \quad n(\tau) = 7\\
\tau(1) = 5 \quad &\Rightarrow \quad \tau = \begin{pmatrix}1&2&3&4&5\\5&2&1&3&4\end{pmatrix} \quad \Rightarrow \quad n(\tau) = 5
\end{aligned}$$

Thus in all cases $n(\tau)$ is odd, meaning that τ is odd and thus cannot belong to A_5.

(vi) Let N be a normal subgroup of the group G, and let the conjugacy class containing g be denoted $C(g)$. Since $g \in C(g)$, we have

$$N \subseteq \bigcup_{n \in N} C(n)$$

Now since "being conjugated" is an equivalence relation, the equivalence classes are clearly either identical or disjoint. It remains to show that if $g \in C(n)$ for some $n \in N$, then $g \in N$. Now if $g \in C(n)$, then there exists an element $h \in G$ such that $g = hnh^{-1}$. This in an element of the set hNh^{-1}, but since N is normal we have $hNh^{-1} = N$ for every $h \in G$. Thus $g \in N$, which shows the inclusion $\supseteq$.

(vii) We are given that A_5 is the disjoint union of conjugacy classes with 1, 12 ,12, 15, and 20 elements, respectively. Now from (vi) above, if A_5 contained a normal subgroup N, it would be the disjoint union of some conjugacy classes. Two more facts are needed to prove the non-existence of such a subgroup: (i) From Lagrange's index theorem, $|N| \mid |A_5| = 5!/2 = 60$. (ii) The conjugacy class containing 1 element must be $C(e) = \{e\}$, and a subgroup always contains e; meaning that $C(e)$ must be included in the union.

Now assume N is a proper normal subgroup. Then $|N|$ is the sum of 1 and some (excluding "all" and "none") of the numbers 12, 12, 15, and 20. If 20 is included in the sum, $|N| \geq 21$, but this means that $|N| = 30$, and 9 cannot be written as a sum of the remaining numbers. Thus 20 cannot be included in the total sum. If 15 is included, we have $|N| \geq 16$, such that $|N| = 20$ or $|N| = 30$, but neither 4 nor 14 may be written as a sum of zero, one or two 12's. Thus 15 cannot be included in the total sum. Finally, if one of the 12's are included, we have $|N| \geq 13$, but neither 13 nor 25 divides 60. Thus we are only left with the possibilities of including all or none of the conjugacy classes; meaning that N must be either A_5 or $\{e\}$, so that A_5 is simple.

Ex. 2.50 Let G be a group, and let $Z(G) = G^G = \{g \in G \mid \forall x \in g\colon gx = xg\}$. Assume $g_1, g_2 \in Z(G)$, and let $x \in G$. Then $g_1g_2x = g_1xg_2 = xg_1g_2$ so that $g_1g_2 \in Z(G)$. Clearly $e \in G$ commutes with every element, so $e \in Z(G)$. Finally, if $g \in Z(G)$, we have $g^{-1}x = g^{-1}xgg^{-1} = g^{-1}gxg^{-1} = xg^{-1}$, so $g^{-1} \in Z(G)$. Thus $Z(G)$ is in fact a subgroup of G. Now since the elements of $Z(G)$ commute with *every* element in G, they certainly commute with each other, so $Z(G)$ is abelian. The same reasoning shows that $hZ(G)h^{-1} = Z(G)$ for every $h \in G$, so $Z(G)$ is normal.

Ex. 2.51 Clearly $H \subseteq N_G(H)$ by §2.1.6 and Exercise 2.1. Now if $g_1, g_2 \in N_G(H)$ we have

$$\begin{aligned}(g_1g_2)H(g_1g_2)^{-1} &= (g_1g_2)H(g_2^{-1}g_1^{-1})\\ &= g_1(g_2Hg_2^{-1})g_1^{-1}\\ &= g_1Hg_1^{-1}\\ &= H,\end{aligned}$$

so $g_1g_2 \in N_G(H)$. Clearly $e \in N_G(H)$ (as already noted, $H \subseteq N_G(H)$). Finally, if $g \in N_G(H)$ then for any $h \in H$ we have $h = gh'g^{-1}$ for some $h' \in H$. Now this implies $g^{-1}hg = h' \in H$, so $g^{-1}Hg \subseteq H$. On the other hand, if $h \in H$ then we may write $h = g^{-1}ghg^{-1}g = g^{-1}h'g$ for some $h' \in H$, so also $H \subseteq g^{-1}Hg$; this proves that $g^{-1} \in N_G(H)$, which is therefore a subgroup of G.

By definition, H is normal if and only if $gHg^{-1} = H$ for every $g \in G$, but this happens by definition if and only if $G = N_G(H)$.

Ex. 2.52 Assume p divides $|G|$. Then we may write $|G| = p^r m$ such that $p \nmid m$ and $r \geq 1$. Now from the First Sylow Theorem, G contains a subgroup H of order p^r. For every $h \in H$, $\operatorname{ord}(h) \mid p^r$. Clearly $p^r > 1$, such that H contains elements other than e. Now choose any element $h \in H$ other than e. If $\operatorname{ord}(h) = p$ we are done. If $\operatorname{ord}(h) \neq p$, we have $\operatorname{ord}(h) = p^s$ where $2 \leq s \leq r$. Then $(h^{p^{s-1}})^p = h^{p^s} = e$, such that $\operatorname{ord}(h^{p^{s-1}})$ divides p. Since $p^{s-1} < p^s$, $h^{p^{s-1}} \neq e$; thus $\operatorname{ord}(h^{p^{s-1}}) \neq 1$, so that $\operatorname{ord}(h^{p^{s-1}}) = p$.

Ex. 2.53 From the First Sylow Theorem, we see that a group G of order $15 = 3 \cdot 5$ has a subgroup of order 3 and a subgroup of order 5. Now from the Third Sylow Theorem, the number of Sylow 3-subgroups divides 5, and vice versa. Thus we have

$$|\mathrm{Syl}_3(G)| \in \{1, 5\}$$
$$|\mathrm{Syl}_5(G)| \in \{1, 3\}$$

Now the Third Sylow Theorem further states that

$$|\mathrm{Syl}_3(G)| \equiv 1 \pmod 3$$
$$|\mathrm{Syl}_5(G)| \equiv 1 \pmod 5$$

from which we see that $|\mathrm{Syl}_3(G)| = |\mathrm{Syl}_5(G)| = 1$. Now since the conditions of Exercise 36(iii) are satisfied (for every divisor d of $|G|$, G contains a unique subgroup of order d), we may conclude that G is cyclic. Another proof is this: Let H_1 be the subgroup of order 3, and H_2 that of order 5. By Exercise 56 below, they are normal. If $x \in H_1 \cap H_2$, then $\operatorname{ord}(x)$ divides both 3 and 5, meaning that $x = e$. Thus $H_1 \cap H_2 = \{e\}$. Now forming the product $H_1 H_2$, we see from Lemma 2.3.7 that it is a subgroup of G. Since $H_1, H_2 \subseteq H_1 H_2$, we have $3 \mid |H_1 H_2|$ and $5 \mid |H_1 H_2|$, so $|H_1 H_2| = 15$; $H_1 H_2 = G$. Thus from Lemma 2.8.1 we have an isomorphism $H_1 \times H_2 \to G$. But since $|H_1| = 3$, it is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, and likewise H_2 is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Thus G is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, which by the Chinese Remainder Theorem (Proposition 2.8.2) again is isomorphic to $\mathbb{Z}/15\mathbb{Z}$. Since the latter is cyclic, so is G.

Ex. 2.54 Consider a regular heptagon K (7-sided polygon). The group G of rotations and reflections mapping K to itself are the rotations with $0, 2\pi/7, 4\pi/7, \ldots, 12\pi/7$ about its center and the reflections in the lines through the center and a vertex. Thus $|G| = 14$. But since G is not abelian (rotating $2\pi/7$, then reflecting in a line L is not the same as first reflecting in L and then rotating $2\pi/7$), G cannot be cyclic, as all cyclic groups are abelian.

Ex. 2.55 Let G be a group of order 20. Any element g of order 5 generates a subgroup of G of order 5. Now from the Third Sylow theorem, we see that

$$|\mathrm{Syl}_5(G)| \text{ divides } 4$$
$$|\mathrm{Syl}_5(G)| \equiv 1 \pmod 5$$

which implies that there is exactly one subgroup H of G of order 5. Since any group of order 5 is cyclic (being isomorphic to $\mathbb{Z}/5\mathbb{Z}$), the four non-trivial elements of H has order 5 in H (and hence in G). There can be no other element of order 5 in G, because such an element would generate a subgroup of order 5 of G different from H, which is impossible.

Ex. 2.56 Since p and q are distinct, the First Sylow Theorem states that G contains a subgroup of order p and a subgroup of order q. Now from the Third Sylow theorem, we may conclude that

$$|\mathrm{Syl}_p(G)| \mid q \Rightarrow |\mathrm{Syl}_p(G)| \in \{1, q\}$$
$$|\mathrm{Syl}_q(G)| \mid p \Rightarrow |\mathrm{Syl}_q(G)| \in \{1, p\}$$

and that

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$$
$$|\mathrm{Syl}_q(G)| \equiv 1 \pmod q$$

Assume WLOG $p > q$. Then p cannot divide $q-1$, so $|\mathrm{Syl}_p(G)| = 1$. The unique subgroup of order p is called H. Now for any $g \in G$, gHg^{-1} is a subgroup of order p, since clearly $e \in gHg^{-1}$; if $x, y \in gHg^{-1}$ then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ so that $xy = gh_1h_2g^{-1}$, and since $h_1h_2 \in H$ we have $xy \in gHg^{-1}$; and finally $x^{-1} = gh_1^{-1}g^{-1}$. Now $|gHg^{-1}| = |H|$ since the map $H \ni x \mapsto gxg^{-1} \in gHx^{-1}$ has the inverse map $x \mapsto g^{-1}xg$. Since there is only one subgroup of order p, we have $gHg^{-1} = H$ for all $g \in G$; thus H is normal. Since $\{e\} \subsetneq H \subsetneq G$, G is not simple.

Chapter 3

Ex. 3.1 Let $x \in R$ be a zero divisor. This means there exists a non-zero element $y \in R$ such that $xy = 0$. If x is a unit, there exists an element $z \in R$ such that $zx = 1$. Thus $y = (zx)y = z(xy) = 0$, using that multiplication is associative. But this contradicts y being non-zero. Thus a zero divisor cannot be a unit, and vice versa.

Ex. 3.2 Assume $\mathbb{R}^3$ may be equipped with a multiplication, such that (writing elements of $\mathbb{R}^3$ as $x + iy + jz$, $x, y, z \in \mathbb{R}$) $i^2 = -1$. Then we may form the product $(0, 1, 0) \cdot (0, 0, 1) = ij = x + iy + jz$, for suitable $x, y, z \in \mathbb{R}$. Multiplying both sides with i (from the left) yields $iij = -j = ix - y + ijz = ix - y + (x + iy + jz)z = x - y + (x + y)i + z^2 j$. But then $z^2 = -1$ for some $z \in \mathbb{R}$, which is impossible. It should be noted that several of the properties (i)–(iii) on page 112 were used, and that multiplication by a real scalar should be commutative.

Ex. 3.3 Using only the rules defining multiplication and addition in a ring, we see that

$$\begin{aligned} 0x &= (0+0)x && \text{Since 0 is the neutral element for +, } 0+0=0 \\ &= 0x + 0x && \text{Property (iii) on page 112 (distributivity)} \end{aligned}$$

But then, using the fact that $(R, +)$ is a group, so that $0x$ has an inverse element $-0x$ with respect to addition, we see that

$$\begin{aligned} 0 &= 0x + (-0x) && \text{Property of } -0x \\ &= (0x + 0x) + (-0x) && \text{The above shown identity } 0x = 0x + 0x \\ &= 0x + (0x + (-0x)) && \text{Associativity of +} \\ &= 0x + 0 && \text{Property of } -0x \\ &= 0x && \text{Property of 0} \end{aligned}$$

To show that $-x$, ie. the additive inverse of x, is equal to $(-1)x$, ie. the additive inverse of 1 multiplied with x, we must show that $(-1)x + x = 0$. This may be shown in a similar fashion to the above:

$$\begin{aligned} (-1)x + x &= (-1)x + 1x \\ &= (-1+1)x \\ &= 0x \\ &= 0. \end{aligned}$$

Strictly speaking, this only shows that $(-1)x$ is *an* additive inverse to x. But the additive group structure of R ensures that there is a unique additive inverse.

Ex. 3.4 Let $I \subseteq R$ be an ideal. Assume $1 \in I$. Then since I is an ideal, we see that for each $\lambda \in R$: $\lambda \cdot 1 = \lambda \in I$; thus $I = R$. Conversely, clearly if $I = R$ then $1 \in I$, since $1 \in R$.

Ex. 3.5 Let $r_1, \ldots, r_n \in R$, and let $\langle r_1, \ldots, r_n \rangle$ denote the set

$$I = \left\{ \sum_{i=1}^{n} \lambda_i r_i \mid \lambda_i \in R \right\}.$$

Then for any two elements $x, x' \in I$ we may write

$$\begin{aligned} x &= \lambda_1 r_1 + \cdots + \lambda_n r_n \\ x' &= \lambda_1' r_1 + \cdots + \lambda_n' r_n \end{aligned}$$

and then

$$x + x' = (\lambda_1 + \lambda_1')r_1 + \cdots + (\lambda_n + \lambda_n')r_n \in I$$

since $\lambda_i + \lambda_i' \in R$ for all i. Clearly $0 \in I$ since $0 = 0r_1 + \cdots + 0r_n$, and $-x = (-\lambda_1)r_1 + \cdots + (-\lambda_n)r_n \in I$. Thus $(I, +)$ is an additive subgroup of $(R, +)$. Now for any $\lambda \in R$, $\lambda x = (\lambda\lambda_1)r_1 + \cdots + (\lambda\lambda_n)r_n \in I$. Thus I is in fact an ideal in R.

Ex. 3.6 Let $I \subseteq R$ be an ideal and $r_1, \ldots, r_n \in I$. Then for any $\lambda_i \in R$ we have $\lambda_i r_i \in I$, and thus any linear combination $\lambda_1 r_1 + \cdots + \lambda_n r_n \in I$, since I is closed under addition. Thus $\langle r_1, \ldots, r_n \rangle \subseteq I$.

Ex. 3.7 Let x_1 and x_2 be any two elements in $I = \langle f \mid f \in M \rangle$. Then we may write

$$\begin{aligned} x_1 &= a_1 f_1 + \cdots + a_m f_m \\ x_2 &= b_1 g_1 + \cdots + b_n g_n \end{aligned}$$

where $f_i, g_i \in M$ and $a_i, b_i \in R$. Then

$$x_1 + x_2 = a_1 f_1 + \cdots + a_m f_m + b_1 g_1 + \cdots + b_n g_n$$

is a finite R-linear combination of elements from M, showing that I is closed under addition. Clearly $0 \in I$, and the additive inverse of x_1 is

$$-x_1 = (-a_1) f_1 + \cdots + (-a_m) f_m$$

so that I is in fact an additive subgroup of R. Now for any $\lambda \in R$ we have

$$\lambda x_1 = (\lambda a_1) f_1 + \cdots + (\lambda a_m) f_m$$

and since $\lambda a_i \in R$ we see that I is closed under multiplication with elements from R.

It should be noted that even if $M = \emptyset$ the ideal is not empty, which is due to the convention that the empty sum in any ring is 0 (ie. $\langle \emptyset \rangle = \{0\}$, the zero ideal).

Ex. 3.8 Let $I, J \subseteq R$ be ideals.

(i) Assume $x_1, x_2 \in I \cap J$. Then $x_1, x_2 \in I$ and $x_1, x_2 \in J$. Since both I and J are ideals, $x_1 + x_2 \in I$ and $x_1 + x_2 \in J$, implying $x_1 + x_2 \in I \cap J$. Clearly $0 \in I$ and $0 \in J$, so that $0 \in I \cap J$. Again using that we may consider I and J as additive groups, we see that $-x_1 \in I$ and $-x_1 \in J$, so that $-x_1 \in I \cap J$. Thus $I \cap J$ is an additive subgroup of R. Now let λ be any element in R. Then $\lambda x_1 \in I$ and $\lambda x_1 \in J$, so that $\lambda x_1 \in I \cap J$. Thus $I \cap J$ is an ideal in R.

(ii) Let x_1 and x_2 be any two elements in $I + J$. Then

$$x_1 = a_1 + b_1 \qquad\qquad x_2 = a_2 + b_2$$

where $a_i \in I$ and $b_i \in J$. Then $x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)$, so that $x_1 + x_2 \in I + J$. Clearly $0 = 0 + 0 \in I + J$, and the additive inverse of x_1 is $(-a_1) + (-b_1)$. Finally, if $\lambda \in R$, we have $\lambda x_1 = \lambda a_1 + \lambda b_1$, and since I and J are ideals, $\lambda x_1 \in I + J$.

(iii) Let x_1 and x_2 be any two elements from IJ. Then we may write

$$x_1 = \sum_{i=1}^{m} a_{1i} b_{1i}$$
$$x_2 = \sum_{i=1}^{n} a_{2i} b_{2i}$$

Then we may write $x_1 + x_2$ as

$$x_1 + x_2 = \sum_{j=1}^{m+n} a_j b_j$$

where $a_j = a_{1j}$ for $1 \leq j \leq m$ and $a_j = a_{2(j-m)}$ for $m+1 \leq j \leq m+n$ (similar for b_j). Thus $x_1 + x_2 \in IJ$. Trivially we have $0 \in IJ$, and

$$-x_1 = \sum_{i=1}^{m} (-a_{1i}) b_{1i} \in IJ.$$

If $\lambda \in R$, then

$$\lambda x_1 = \sum_{i=1}^{m} (\lambda a_{1i}) b_{1i} \in IJ.$$

Thus IJ is in fact an ideal in R.

If one of I and J is a principal ideal, one may prove that $\{ab \mid a \in I, b \in J\}$ is an ideal in R. This is certainly the case if R is a PID (see Definition 3.1.9). To find a counterexample showing that $\{ab \mid a \in I, b \in J\}$ we thus need to find two ideals in a ring which is not a PID.

(iv) Let $x \in IJ$. Then x is a linear combination of elements from I and J;

$$x = \sum_{i=1}^{n} a_i b_i.$$

Now since I is an ideal, and $a_i \in I$, we have $a_i b_i \in I$ for all i (using that an ideal is closed under multiplication with any element from R). Similarly J is an ideal, and $b_i \in J$, so we have $a_i b_i \in J$ for all i. Thus $a_i b_i \in I \cap J$ for all i. From (i), $I \cap J$ is an ideal, and is thus closed under addition, so that

$$\sum_{i=1}^{n} a_i b_i \in I \cap J,$$

thus $IJ \subseteq I \cap J$. Let $I = J = 2\mathbb{Z} \subseteq \mathbb{Z}$. Then clearly $I \cap J = 2\mathbb{Z}$, and $IJ = 4\mathbb{Z}$ (any linear combination of products of elements from I and I is a multiple of 4), so that $IJ \subseteq I \cap J$ but $IJ \neq I \cap J$.

(v) The answer is no. As mentioned above a counterexample necessarily involves a ring which is not a PID. A good candidate is the (in fact also non-UFD) ring $R = \mathbb{Z}[\sqrt{-5}]$. Let $I = J = \langle 2, 1 + \sqrt{-5} \rangle \subseteq R$, and define the set

$$A = \{ab \mid a, b \in I\}.$$

We wish to show that A is not an ideal in R.

Since $2 \in I$ we have $4 = 2 \cdot 2 \in A$. Since $1-\sqrt{-5} = -(1+\sqrt{-5})+2 \in I$ we also have $6 = (1+\sqrt{-5})(1-\sqrt{-5}) \in A$. Assuming A is an ideal, this means that $2 = 6-4 \in A$. But then $2 = ab$, where $a, b \in I$. Since 2 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$ (see Remark 3.5.4) this means that either a or b is a unit. Since $I \neq R$ (see Remark 3.5.8) we have a contradiction, so A cannot be an ideal.

Ex. 3.9 Assume

$$x_1, x_2 \in \bigcup_{n=1}^{\infty} I_n.$$

Then $x_1 \in I_i$ and $x_2 \in I_j$ for some i, j. We may WLOG assume that $j \geq i$. Since the sequence of ideals is increasing, we have $I_i \subseteq I_j$, meaning that $x_1 \in I_j$. Then $x_1 + x_2 \in I_j$, so that $x_1 + x_2 \in \bigcup_{n=1}^{\infty} I_n$. Clearly 0 belongs to the union of the ideals, and $-x_1 \in I_i \subseteq \bigcup_{n=1}^{\infty} I_n$. Further, if λ is any element in R, $\lambda x_1 \in I_i \subseteq \bigcup_{n=1}^{\infty} I_n$. This shows that the union is in fact an ideal. The only "tricky" part was showing that it is closed under addition. This gives an idea to finding two ideals I and J such that $I \cup J$ is not an ideal. Consider the ideals $I = 2\mathbb{Z}$ and $J = 3\mathbb{Z}$ in the ring $\mathbb{Z}$. Then $2, 3 \in I \cup J$, but $2+3 = 5$ is not an element in either of $2\mathbb{Z}$ and $3\mathbb{Z}$, so $I \cup J$ is not closed under addition; thus not an ideal.

Ex. 3.10 (i) From Exercise 9 above, we know that

$$I = \bigcup_{n=1}^{\infty} I_n$$

is an ideal in R. By assumption we may find $r_1, \ldots, r_k \in R$ such that

$$I = \langle r_1, \ldots, r_k \rangle.$$

Now let $N_i = \min\{n \mid r_i \in I_n\}$, ie. the index of the "first" ideal containing the i'th generator (such an index must exist, since $r_i \in \bigcup I_n$). Let $N = \max_i\{N_i\}$. Then we must have $I = I_N = I_{N+1} = \cdots$. This follows from the fact that $I_N, I_{N+1}, \ldots$ contain $r_1, \ldots, r_k$, and therefore they contain all R-linear combinations of the generators of I. Thus they contain all elements of I. The other inclusions are trivial from the definition of I. Thus the sequence of ideals stabilize after a finite number of steps.

(ii) Let J be any ideal $\neq R$ in the noetherian ring R. Then there exists a maximal ideal containing J:

If J is a maximal ideal we are done. If not, we may find an ideal $I_1 \neq R$ such that $J \subseteq I_1$. If I_1 is a maximal ideal, we are done. Continuing this way, we obtain a sequence

$$J \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

and from (i) this sequence must stabilize. Thus J is contained in the ideal I_N, which by construction is a maximal ideal.

Ex. 3.11 Let $f\colon R \to S$ be a ring homomorphism. Let $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$. If $x, y \in \operatorname{Ker} f$ then $f(x+y) = f(x) + f(y) = 0 + 0 = 0$; thus $x + y \in \operatorname{Ker} f$. Since $f(0) = 0$ we have $0 \in \operatorname{Ker} f$, and $f(-x) = -f(x) = 0$. Finally for any $\lambda \in R$ we have $f(\lambda x) = f(\lambda)f(x) = f(\lambda) \cdot 0 = 0$, so $\lambda x \in \operatorname{Ker} f$. Thus $\operatorname{Ker} f$ is an ideal.

From the definition of a ring homomorphism, $0 = f(0)$ and $1 = f(1)$, such that $0, 1 \in f(R)$. Now let $s_1, s_2 \in f(R)$. This means $s_1 = f(r_1)$ and $s_2 = f(r_2)$ for suitable $r_i \in R$. Then $s_1 + s_2 = f(r_1) + f(r_2) = f(r_1 + r_2) \in f(R)$, $-s_1 = -f(r_1) = f(-r_1) \in f(R)$, and finally $s_1 s_2 = f(r_1)f(r_2) = f(r_1 r_2) \in f(R)$; thus $f(R) \subseteq S$ is a subring.

Ex. 3.12 (i) As in Example 1.5.3, we may find (λ, μ) by this sequence of calculations

$$\begin{aligned}
49 &= 1 \cdot 49 + 0 \cdot 13\\
13 &= 0 \cdot 49 + 1 \cdot 13\\
10 &= 1 \cdot 49 - 3 \cdot 13\\
3 &= 1 \cdot 13 - 1 \cdot 10\\
&= -1 \cdot 49 + 4 \cdot 13\\
1 &= 1 \cdot 10 - 3 \cdot 3\\
&= 4 \cdot 49 - 15 \cdot 13
\end{aligned}$$

or using a table such as in Example 1.5.5

i	-1	0	1	2	3
r_i	49	13	10	3	1
q_i			3	1	3
a_i	1	0	1	-1	4
b_i	0	1	-3	4	-15

Thus we may choose $(\lambda, \mu) = (4, -15)$. From this we see that

$$\begin{aligned}[-15][13] &= [-15 \cdot 13] \\ &= [1 - 4 \cdot 49] \\ &= [[1] - [4 \cdot 49]] \\ &= [1],\end{aligned}$$

where $[\,\cdot\,]$ denotes congruence class modulo 49. Thus $[13]$ is a unit in $\mathbb{Z}/49\mathbb{Z}$ (with inverse $[-15] = [34]$).

(ii) Let R denote the ring $\mathbb{Z}/p^l\mathbb{Z}$, where p is a prime number and $l > 0$. If $l > 1$, we have $[p] \neq [0]$, $[p^{l-1}] \neq [0]$, but $[p][p^{l-1}] = [p^l] = [0]$, so that R contains at least one zero divisor, and is thus not a domain.

(iii) The units in R are exactly the residue classes $[m]$ where $\gcd(m, p^l) = 1$; thus the number of units in R is $|R^*| = \varphi(p^l) = p^l - p^{l-1}$ by §2.3.2. The number of non-units is therefore $|R| - |R^*| = p^{l-1}$.

(iv) Assume $r = r^2$ for some $r \in R$. Let $r = [x]$ for a suitable $0 \leq x < p^l$. Then $r^2 - r = [x^2 - x] = [x(x-1)] = [0]$, which means $x(x-1)$ is a multiple of p^l. Then p^l divides $x(x-1)$, and since p cannot divide both x and $x-1$, p^l must divide either x or $x-1$. If p^l divides x, then $x = 0$, since $0 \leq x < p^l$, and if p^l divides $x-1$, $x = 1$ since $-1 \leq x-1 < p^l - 1$. Thus $r^2 = r$ if and only if $r = [0]$ or $r = [1]$.

Ex. 3.13 The group of units in the ring of Gaussian integers $\mathbb{Z}[i]$ is $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$. It is easily verified that $\mathbb{Z}[i]^*$ is a cyclic group (for instance generated by i), and since cyclic groups of the same order are always isomorphic, $\mathbb{Z}[i]^*$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. The claim may be proved as follows: Let A be any cyclic group, with generator a. Then the map $\varphi\colon \mathbb{Z} \to A$ given by $\varphi(n) = a^n$ is clearly surjective (since A is generated by a). The kernel $\operatorname{Ker}\varphi$ is a subgroup of $\mathbb{Z}$, and is thus of the form $N\mathbb{Z}$. From the isomorphism theorem for groups we see that A is isomorphic to $\mathbb{Z}/N\mathbb{Z}$. If B is another cyclic group, by a similar argument it is isomorphic to $\mathbb{Z}/M\mathbb{Z}$, and if A and B have the same order, we must have $M = N$. Thus if A and B are cyclic groups of the same order (be it finite or countably infinite), they are isomorphic to the same group, and are therefore isomorphic.

Ex. 3.14 Let $\omega = e^{2\pi i/p}$ where p is an integer > 1. Define

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} \mid a_i \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

If $x, y \in \mathbb{Z}[\omega]$ then clearly $x + y \in \mathbb{Z}[\omega]$, $-x \in \mathbb{Z}[\omega]$ and $0 \in \mathbb{Z}[\omega]$, so $\mathbb{Z}[\omega]$ is an additive subgroup of $\mathbb{C}$. Clearly also $1 \in \mathbb{Z}[\omega]$. Finally

$$\begin{aligned}
xy &= (a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2})(b_0 + b_1\omega + \cdots + b_{p-2}\omega^{p-2}) \\
&= a_0b_0 + a_0b_1\omega + \ldots a_0b_{p-2}\omega^{p-2} \\
&+ a_1b_0\omega + a_1b_1\omega^2 + \cdots + a_1b_{p-2}\omega^{p-1} \\
&\vdots \\
&+ a_{p-2}b_0\omega^{p-2} + a_{p-2}b_1\omega^{p-1} + \cdots + a_{p-2}b_{p-2}\omega^{2p-4}
\end{aligned}$$

Thus xy is a $\mathbb{Z}$-linear combination of integer powers of ω. Since $\omega^p = e^{2\pi i} = 1$, and $\omega^j \in \mathbb{Z}[\omega]$ for all $0 \leq j \leq p-2$, it only remains to show that $\omega^{p-1} \in \mathbb{Z}[\omega]$. This follows from the fact that

$$\begin{aligned}
1 + \omega + \cdots + \omega^{p-1} &= \sum_{j=0}^{p-1} \omega^j \\
&= \frac{1-\omega^p}{1-\omega} \\
&= 0
\end{aligned}$$

so that

$$\omega^{p-1} = -1 - \omega - \cdots - \omega^{p-2} \in \mathbb{Z}[\omega].$$

Ex. 3.15 (i) Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. It is clearly an additive subgroup of $(\mathbb{R}, +)$, and $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Now for $x, y \in \mathbb{Z}[\sqrt{2}]$ we have $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, and $xy = ac + 2bd + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, which is therefore a subring of $\mathbb{R}$.

(ii) Since $(1+\sqrt{2})(-1+\sqrt{2}) = 2 - 1 = 1$, $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. Then any positive power of $1 + \sqrt{2}$ is a unit (the inverse being $(-1+\sqrt{2})^n$), and since $1 + \sqrt{2} > 1$ the set $\{(1+\sqrt{2})^n \mid n \in \mathbb{N}\}$ is infinite; since it is a subset of $\mathbb{Z}[\sqrt{2}]^*$ the latter is also infinite. One may even prove that all units in $\mathbb{Z}[\sqrt{2}]$ are of the form $\pm(1+\sqrt{2})^n$ where $n \in \mathbb{Z}$; in other words the group of units is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ex. 3.16 Let R denote the ring $\mathbb{Z}[i]/\langle 1 + 3i\rangle$.

(i) We have $i - 3 = i(1 + 3i) \in \langle 1 + 3i\rangle$. Then $[i - 3] = [0]$ in R and consequently $[i] = [3]$. Squaring both sides we see that $[i]^2 = [i^2] = [-1] = [3]^2 = [9]$, so that $[0] = [10]$ in R. For any $a, b \in \mathbb{Z}$ we have $[a + bi] = [a] + [bi] = [a] + [b][i] = [a] + [b][3] = [a + 3b]$.

(ii) The unique ring homomorphism $\varphi\colon \mathbb{Z} \to R$ must necessarily send $x \in \mathbb{Z}$ to $[x]$. Then since $[a + bi] = [a + 3b]$, we see that $\varphi(a + 3b) = [a + bi]$, which shows that φ is surjective.

(iii) Let $N\colon \mathbb{Z}[i] \to \mathbb{N}$ denote the usual norm function, $N(a + bi) = a^2 + b^2$. Then as usual $N(xy) = N(x)N(y)$. Assuming $1+3i$ is a unit, it has an inverse $a + bi$. Then $1 = N(1) = N((1 + 3i)(a + bi)) = 10N(a + bi) = 10(a^2 + b^2)$. This is impossible, since $a, b \in \mathbb{Z}$; thus $1 + 3i$ is not a unit (the complete set of units in $\mathbb{Z}[i]$ was in fact found in Example 3.1.5). Similarly if $1 + 3i$ divides 2, respectively 5, there exists integers a, b such that $N((1 + 3i)(a + bi)) = 10(a^2 + b^2)$ equals 4, respectively 25, which in both cases is impossible. Since φ is a ring homomorphism, $\operatorname{Ker}\varphi$ is an ideal in $\mathbb{Z}$. Thus $\operatorname{Ker}\varphi = d\mathbb{Z}$ for some $d \in \mathbb{N}$. Clearly $10\mathbb{Z} \subseteq \operatorname{Ker}\varphi$ since $\varphi(10) = [0]$. Since $1 + 3i$ does not divide 1, 2 or 5, $1, 2, 5 \notin \langle 1 + 3i\rangle$, and thus $\varphi(1), \varphi(2), \varphi(5)$ are all different from $[0]$ in R. Thus $\operatorname{Ker}\varphi = 10\mathbb{Z}$.

(iv) Since φ is surjective with kernel $10\mathbb{Z}$, it follows from Proposition 3.3.2 that $\mathbb{Z}/10\mathbb{Z}$ is isomorphic to R.

Ex. 3.17 Let R be a commutative ring, and let $I \subseteq J$ be ideals in R.

(i) Define $\varphi\colon R/I \to R/J$ by $\varphi(x + I) = x + J$. It is well-defined, for if $x + I = x' + I$, we have $x - x' \in I$; thus $x - x' \in J$ and therefore $x + J = x' + J$. Let $x + J \in R/J$. Then $R/I \ni x + I \overset{\varphi}{\mapsto} x + J$, which shows that φ is surjective.

φ is a group homomorphism from $(R/I, +)$ to $(R/J, +)$, since

$$\begin{aligned}\varphi((x_1 + I) + (x_2 + I)) &= \varphi((x_1 + x_2) + I)\\ &= (x_1 + x_2) + J\\ &= (x_1 + J) + (x_2 + J)\end{aligned}$$

by the definition of addition in a quotient ring. Similarly by the definition of multiplication in a quotient ring we obtain

$$\begin{aligned}\varphi((x_1 + I)(x_2 + I)) &= \varphi((x_1x_2) + I)\\ &= (x_1x_2) + J\\ &= (x_1 + J)(x_2 + J).\end{aligned}$$

Finally we have $\varphi(1 + I) = 1 + J$; ie. the neutral element for multiplication in R/I is mapped to the neutral element for multiplication in R/J. Thus φ is in fact a ring homomorphism.

(ii) Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Let $n \in \mathbb{Z} \setminus \{0\}$ and the ideal $I = Rn \subseteq R$. Assume $a + bi \in I$. Then there exists integers x and y such that $a + bi = (x + yi)n = xn + yni$ from which $a = xn$ and $b = yn$; ie. $n \mid a$ and $n \mid b$. If conversely $n \mid a, b$ we have integers x, y satisfying $a + bi = xn + yni \in I$.

Now assume the quotient ring R/I is infinite. Then we may certainly choose n^2+1 different elements $x_0, x_1, \dots, x_{n^2}$. Let $x_j = [a_j + b_j i]$. Then among the $n^2 + 1$ pairs $\{(a_j, b_j)\}$ there must be two pairs (a_j, b_j) and (a_k, b_k) with $a_j \equiv a_k \pmod{n}$ and $b_j \equiv b_k \pmod{n}$ by the pigeon hole principle, since there are only n^2 different elements in $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. Now this implies $x_j - x_k = [(a_j - a_k) + (b_j - b_k)i]$; but this is equal to $[0]$; ie. $x_j = x_k$ contrary to the hypothesis.

(iii) Let $J \neq \{0\}$ be an ideal in R. Then clearly $J \cap \mathbb{Z}$ is non-empty, since $0 \in \mathbb{Z}$ and $0 \in J$. Furthermore, since J contains at least one element z different from 0, it also contains the element $z\bar{z} = |z|^2$ (since J is an ideal); thus $|z|^2 \in J \cap \mathbb{Z}$, and $|z|^2 \neq 0$.

Now let $x_1, x_2 \in J \cap \mathbb{Z}$. Then since both J and $\mathbb{Z}$ may be considered as additive groups, $x_1 + x_2 \in J \cap \mathbb{Z}$ and $-x_1 \in J \cap \mathbb{Z}$. Thus $J \cap \mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$; and these are exactly the ideals in $\mathbb{Z}$.

(iv) From (iii), $J \cap \mathbb{Z} = d\mathbb{Z}$ for some $d > 0$. Let I denote the ideal $\langle d \rangle \subseteq R$. For $z \in I$ we have $z = xd + ydi$. Since $xd, yd \in d\mathbb{Z} \subseteq J$ and since J is an ideal in R, we have $xd, ydi \in J$; thus $z = xd + ydi \in J$. Thus $I \subseteq J$, and from (i) we have a surjective mapping from R/I to R/J. From (ii), R/I is finite, which implies that R/J is finite.

Ex. 3.18 Let R be a ring of characteristic zero. Let $f\colon \mathbb{Z} \to R$ be the unique ring homomorphism, and let $S = f(\mathbb{Z}) \subseteq R$. By Exercise 3.11 S is a subring of R. Since $\operatorname{char} R = 0$, there are no integers > 0 for which $f(n) = 0$; thus $\operatorname{Ker} f = \{0\}$. This immediately implies $S \cong \mathbb{Z}/0\mathbb{Z}$, but since the latter is clearly isomorphic to $\mathbb{Z}$, we see that $S \cong \mathbb{Z}$.

Ex. 3.19 Let $\varphi\colon R \to S$ be a ring homomorphism. First assume S is a domain. Then by Exercise 3.11 $\varphi(R)$ is a subring of S, and must also be a domain. By the isomorphism theorem for rings, $R/\operatorname{Ker}\varphi$ is isomorphic to $f(R)$; thus $R/\operatorname{Ker}\varphi$ is itself a domain, and by Proposition 3.2.6 $\operatorname{Ker}\varphi$ is a prime ideal. Now assume S is a field and φ is surjective. Then $\varphi(R) = S$ and $R/\operatorname{Ker}\varphi \cong S$; thus $R/\operatorname{Ker}\varphi$ is a field and by Proposition 3.2.7 $\operatorname{Ker}\varphi$ is a maximal ideal.

Ex. 3.20 Let I be an ideal in the ring R and let $\pi\colon R \to R/I$ denote the canonical ring homomorphism.

(i) Let $J \subseteq R/I$ be an ideal. We wish to show that the preimage $\pi^{-1}(J)$ is an ideal in R containing I. For any element $y \in I$ we have $\pi(y) = [0] \in R/I$, and since J is an ideal, $[0] \in J$; thus $I \subseteq \pi^{-1}(J)$. Now let $x_1, x_2 \in \pi^{-1}(J)$. Then $\pi(x_1), \pi(x_2) \in J$, and $\pi(x_1 + x_2) = \pi(x_1) + \pi(x_2) \in J$; thus $x_1 + x_2 \in \pi^{-1}(J)$. Since $0 \in I$, $0 \in \pi^{-1}(J)$. Also $-x_1 \in \pi^{-1}(J)$ since $\pi(-x_1) = -\pi(x_1) \in J$. Finally, if $\lambda \in R$ is any element, $\pi(\lambda x_1) = \pi(\lambda)\pi(x_1) \in J$, since $\pi(\lambda)$ is some element in R/I and J is an ideal in R/I.

(ii) Let $I' \supseteq I$ be an ideal containing I. Let $y_1, y_2 \in \pi(I')$. Then $y_1 = \pi(x_1)$ and $y_2 = \pi(x_2)$ for some $x_1, x_2 \in I'$. Then $y_1 + y_2 = \pi(x_1) + \pi(x_2) = \pi(x_1 + x_2) \in \pi(I')$. Clearly $[0] = \pi(0) \in \pi(I')$, and $-y_1 = -\pi(x_1) = \pi(-x_1) \in \pi(I')$. If $\alpha \in R/I$, then $\alpha = \pi(\lambda)$ for some $\lambda \in R$ (since π is surjective). Thus $\alpha y_1 = \pi(\lambda)\pi(x_1) = \pi(\lambda x_1) \in \pi(I')$, since $\lambda x_1 \in I'$. Thus $\pi(I')$ is an ideal in R/I.

(iii) We wish to show that

$$\pi\colon \{\text{ideals in } R \text{ containing } I\} \to \{\text{ideals in } R/I\} \tag{3.1}$$

is a bijection. This amounts to showing that

$$\pi^{-1}(\pi(I')) = I' \tag{3.2}$$

$$\pi(\pi^{-1}(J)) = J \tag{3.3}$$

whenever I' is an ideal in R containing I and J is an ideal in R/I. One easily verifies the inclusion $\supseteq$ in the first equation. Now assume $x \in \pi^{-1}(\pi(I'))$. Then $\pi(x) \in \pi(I')$. Thus for some $x' \in I'$ we have $x + I = x' + I$, implying $x - x' \in I \subseteq I'$. Then since I' is an ideal we have $x = (x - x') + x' \in I'$, which shows (3.2).

As above, one may easily verify the inclusion $\subseteq$ in (3.3). Assume $y \in J$. Then $y = x + I$ for some $x \in R$, and $x \in \pi^{-1}(\{y\}) \subseteq \pi^{-1}(J)$. Then $y = \pi(x) \in \pi(\pi^{-1}(J))$. Thus π considered as the mapping in (3.1) is a bijection. That π and π^{-1} preserves $\subseteq$ follows from general facts about mappings between sets of sets.

If R/I is a field, then there are no other ideals than $\langle [0] \rangle$ and R/I (see Remark 3.1.8). By the above, this shows that there are only two ideals in R containing I; namely I and R, respectively. Thus I is a maximal ideal.

Conversely, if I is a maximal ideal, the only ideals in R containing I are I and R. This shows that the only ideals in R/I are $\langle [0] \rangle$ and R/I. So if x is a non-zero element in R/I then $\langle x \rangle = R/I$, so there exists $y \in R/I$ such that $xy = 1$. This shows that R/I is a field.

(iv) Since there is a bijective correspondence between ideals in $\mathbb{Z}/24\mathbb{Z}$ and ideals in $\mathbb{Z}$ containing $24\mathbb{Z}$, we may find the former by applying the canonical ring homomorphism to the latter. The ideals in $\mathbb{Z}$ containing $24\mathbb{Z}$ are

$$\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 8\mathbb{Z}, 12\mathbb{Z}, \text{ and } 24\mathbb{Z},$$

corresponding to the following set of ideals in $\mathbb{Z}/24\mathbb{Z}$:

$$\{\mathbb{Z}/24\mathbb{Z}, \langle[2]\rangle, \langle[3]\rangle, \ldots, \langle[0]\rangle\}.$$

Ex. 3.21 Let R be a non-zero commutative ring and $P \subseteq R$ a prime ideal. Let $[x], [y] \in R/P$, and assume $[xy] = [0]$. Then $xy \in P$, and since P is a prime ideal this implies $x \in P$ or $y \in P$; thus $[x] = [0]$ or $[y] = [0]$ in R/P, and R/P is a domain.

Ex. 3.22 Let I and J be ideals and P a prime ideal in the ring R. Assume $IJ \subseteq P$. The ideal IJ is (cf. Exercise 3.8(iii)) defined as

$$IJ = \{\sum_{i=1}^{n} a_i b_i \mid n \geq 1, a_i \in I, b_i \in J\}.$$

Thus we may conclude that for all $a \in I$ and all $b \in J$ that

$$ab \in IJ \subseteq P,$$

and since P is a prime ideal we have $a \in P$ or $b \in P$ by §3.2.2. If $\forall a \in I\colon a \in P$ we are done, for then $I \subseteq P$. If this is not the case, then there is an $a' \in I$ such that $a' \notin P$. Then for all $b \in J$ we have $a'b \in P$, which implies $b \in P$ (because at least one of a' and b belong to P); thus $J \subseteq P$.

Ex. 3.23 Let F be a finite domain. We wish to show that for every $x \in F \setminus \{0\}$ there exists an element $y \in F$ such that $xy = 1$. Consider $x, x^2, x^3, \ldots$. Since F is a domain and x is non-zero, every element in this sequence is non-zero (otherwise x would be a zero divisor). Since F is finite, there must be two exponents $m < n$ such that $x^m = x^n$. Then $x^{n-m}x^m = x^{n-m}x^n = x^n$; thus since F is a domain and x^n is non-zero we have $x^{n-m} = 1$. But then $1 = x \cdot x^{n-m-1}$; and x is a unit with inverse x^{n-m-1} (notice that $n-m-1 \geq 0$).

Ex. 3.24 If F is a field and Q is the "field of fractions" for F as defined in §3.4, we wish to show that F and Q are isomorphic. A natural candidate for an isomorphism is the inclusion map $i\colon F \to Q$, $i(x) = \frac{x}{1}$. As stated in §3.4, this is an injective ring homomorphism, so it only remains to show that i is surjective. Let $a = \frac{x}{y} \in Q$. Then since F is a field and $y \neq 0$, there exists $y^{-1} \in F$, and $a = i(x)i(y^{-1}) = i(xy^{-1})$. Thus $F \cong Q$ and we might as well consider F and Q the same.

Ex. 3.25 Let R be a PID, and let $I \subseteq R$ be an ideal in R. Then I is generated by a single element, $I = \langle a \rangle$. Let J be an ideal in the quotient ring R/I. By Exercise 20, $I' = \pi^{-1}(J)$ is an ideal in R containing I. Then I' is a principal ideal, and we may write $I' = \langle a' \rangle$. The only natural candidate for a generator for J is $b = \pi(a')$. Since $a' \in \pi^{-1}(J)$ we have $b \in J$, so $\langle b \rangle \subseteq J$. Now let $x \in J$, and consider the subset $\pi^{-1}(x) \subseteq I'$. It is non-empty, since π is surjective. Choose a $c \in \pi^{-1}(x)$. Then since a' generates I' we have $c = \lambda a'$ for some $\lambda \in R$. But then $x = \pi(c) = \pi(\lambda)\pi(a') = \pi(\lambda)b \in \langle b \rangle$, showing that $J \subseteq \langle b \rangle$. Thus J is a principal ideal.

Since $\mathbb{Z}$ is a principal ideal domain, every ideal in the quotient ring $\mathbb{Z}/4\mathbb{Z}$ is a principal ideal. But $\mathbb{Z}/4\mathbb{Z}$ is not a domain (since $[2][2] = [0]$ and $[2] \neq [0]$).

Ex. 3.26 The units in $\mathbb{Z}/8\mathbb{Z}$ are $\mathbb{Z}/8\mathbb{Z}^* = \{[1], [3], [5], [7]\}$, and each of these is its own inverse.

Consider the product ring $R = \mathbb{Z} \times \mathbb{Z}$ with componentwise addition and multiplication. Then $(1, 0) \in R$ is an idempotent element different from $(0, 0)$ and $(1, 1)$.

The non-commutative ring $\mathrm{Mat}_2(\mathbb{R})$ of 2×2-matrices with real entries is another example of a ring with an idempotent element different from 0 and 1 (for instance $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$).

If R is any ring with such an element, $x(x-1) = 0$, and since x is assumed to be different from 0 and 1, x is a zero divisor so R is not a domain. If $x^2 = x$ for all $x \in R$, then $x(x-1) = 0$ for all x. Using this fact for $x = 1 + 1$ one sees that $(1+1)(1+1-1) = (1+1) \cdot 1 = 0$; thus $1 + 1 = 0$ and $\operatorname{char} R = 2$. (In fact, this is only true if one assumes that R is not the zero ring).

Ex. 3.27 It is well-known that complex conjugation satisfies $\overline{z+w} = \bar{z} + \bar{w}$ and $\overline{zw} = \bar{z}\bar{w}$. Clearly also $\bar{1} = 1$, so $f(z) = \bar{z}$ is in fact a ring homomorphism $\mathbb{Z}[i] \to \mathbb{Z}[i]$. Assume $\pi \in \mathbb{Z}[i]$ is a prime element, and that $f(\pi) \mid ab$. Then there is an $x \in \mathbb{Z}[i]$ such that $x\bar{\pi} = ab$, implying $\bar{x}\pi = \bar{a}\bar{b}$. Then $\pi \mid \bar{a}\bar{b}$, and since π is a prime element, this implies $\pi \mid \bar{a}$ or $\pi \mid \bar{b}$. Assume WLOG $\pi \mid \bar{a}$. Then there is an element $y \in \mathbb{Z}[i]$ such that $y\pi = \bar{a}$, from which $\bar{y}\bar{\pi} = a$. Finally we see that $f(\pi) \mid a$, so that $f(\pi)$ is in fact a prime element.

Ex. 3.28 The remainder need not be unique; as a simple example consider the Euclidean domain $R = \mathbb{Z}[i]$ with the usual norm function. Let $x = 2 + 2i$ and $d = 1 + 2i$. Then $N(d) = 5$, and $x = 1 \cdot d + 1 = 2 \cdot d - 2i$; both 1 and $-2i$ are valid as remainders. An even simpler example is $8 = 2 \cdot 3 + 2 = 3 \cdot 3 - 1$ within $\mathbb{Z}$; if one uses the absolute value $|\cdot|$ as a Euclidean function both 2 and -1 qualify as remainders after division by 3.

Ex. 3.29 Let $a = 4 + 5i$ and $b = 7 + 8i$. Then a table as the one below may easily be built. One may check that $(\lambda, \mu) = (5 - 2i, -3 + i)$ computed as in

a	b	$N(a)$	$N(b)$	q	r	$N(r)$
$4+5i$	$7+8i$	41	113	1	$3+3i$	18
$3+3i$	$4+5i$	18	41	1	$1+2i$	5
$1+2i$	$3+3i$	5	18	$1-i$	$2i$	4
$2i$	$1+2i$	4	5	1	1	1
1	$2i$	1	4	$2i$	0	
0	1					

Table 1: The Euclidean algorithm in $\mathbb{Z}[i]$

Example 1.5.3 satisfies $\lambda a + \mu b = 1$.

Ex. 3.30 Let $\mathbb{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbb{Z}\}$ where $\omega^2 + \omega + 1 = 0$. Let $z = x + y\omega$ be an element in $\mathbb{Z}[\omega]$.

(i) Since both ω and $\bar{\omega}$ satisfy the quadratic equation defining ω, we have $X^2 + X + 1 = (X - \omega)(X - \bar{\omega})$; hence $\omega\bar{\omega} = 1$ and $\omega + \bar{\omega} = -1$, so

$$\begin{aligned} N(z) &= z\bar{z} \\ &= (x + y\omega)(\overline{x + y\omega}) \\ &= (x + y\omega)(x + y\bar{\omega}) \\ &= x^2 + xy(\omega + \bar{\omega}) + y^2\omega\bar{\omega} \\ &= x^2 - xy + y^2 \end{aligned}$$

If $z_1 = x_1 + y_1\omega$ and $z_2 = x_2 + y_2\omega$, then

$$\begin{aligned} N(z_1z_2) &= z_1z_2\overline{z_1z_2} \\ &= z_1\bar{z}_1z_2\bar{z}_2 \\ &= N(z_1)N(z_2) \end{aligned}$$

Assume $z = x + y\omega \in \mathbb{Z}[\omega]$ is a unit. Then there exists a $w = u + v\omega$ such that $zw = 1$. Then $N(zw) = N(z)N(w) = 1$. Both factors are positive integers; hence $N(z) = 1$. Now assume $N(z) = 1$. This means $z\bar{z} = 1$, so in order to show that z is a unit one only has to show that $\bar{z} \in \mathbb{Z}[\omega]$. But $\bar{z} = \overline{x + y\omega} = x + y\bar{\omega}$, so what remains is to show that $\bar{\omega} \in \mathbb{Z}[\omega]$. But since $\omega + \bar{\omega} = -1$ we have $\bar{\omega} = -1 - \omega \in \mathbb{Z}[\omega]$ (notice that this is completely independent of whether we think of ω as $-\frac{1}{2} + \frac{\sqrt{3}}{2}$ or $-\frac{1}{2} - \frac{\sqrt{3}}{2}$).

(ii) Assume $N(z)$ is a prime number, and that $z = ab$. Then $N(z) = N(a)N(b)$, and since $N(z)$ is prime, one of $N(a)$ and $N(b)$ must equal 1. Thus either a or b is a unit, so z is irreducible.

(iii) Let $z, d \in \mathbb{Z}[\omega]$, $d \neq 0$. If d divides z, then $z = qd$ for some $q \in \mathbb{Z}[\omega]$. If not, $z - qd \neq 0$ for every $q \in \mathbb{Z}[\omega]$. It is geometrically obvious that no point in the complex plane has a distance to $\mathbb{Z}[\omega]$ which is larger than 1. To see this, one only has to consider points inside the parallelogram with vertices 0, 1, ω and $1 + \omega$ (because of translational symmetry). Now the vertices 1, ω and $1+\omega$ all lie on the unit circle, so no point on or in the interior of the parallelogram has a distance to 0 that is greater than 1; so certainly the distance to the nearest vertex is < 1.

Consider the complex number $\frac{z}{d}$. The above observation means that we may find a $q \in \mathbb{Z}[\omega]$ such that $|\frac{z}{d} - q| < 1$. Let $r = z - qd$. Then $z = qd + r$, and since

$$\begin{aligned} \tfrac{N(r)}{N(d)} &= |\tfrac{z-qd}{d}|^2 \\ &= |\tfrac{z}{d} - q|^2 \\ &< 1 \end{aligned}$$

we have $N(r) < N(d)$. Thus $N\colon \mathbb{Z}[\omega] \to \mathbb{N}$ is a Euclidean function.

(iv) Since $\mathbb{Z}[\omega]$ is a Euclidean domain, it is a PID (Theorem 3.5.9), and thus a UFD (Theorem 3.5.7). Lemma 3.5.5 and Proposition 3.5.3 then states that in $\mathbb{Z}[\omega]$ the prime elements are exactly the irreducible elements, and since $N(1-\omega) = 1+1+1 = 3$ is a prime number, $1-\omega$ is irreducible (by (ii)) and thus a prime element of $\mathbb{Z}[\omega]$.

Ex. 3.31 In $\mathbb{Z}[\sqrt{-3}]$ we may factor 4 as both $2 \cdot 2$ and $(1+\sqrt{-3})(1-\sqrt{-3})$. Now all of $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ are irreducible in $\mathbb{Z}[\sqrt{-3}]$, because if x denotes any of these elements and $x = ab$, we have $4 = N(x) = N(a)N(b) = (a_1^2 + 3a_2^2)(b_1^2 + 3b_2^2)$ implying that one of $N(a)$ and $N(b)$ is equal to 1; which again implies that one of a and b is a unit.

Since 2 does not divide $1 \pm \sqrt{-3}$ (this would imply $2 \mid 1$ within $\mathbb{Z}$, which is impossible), these factorizations are essentially different. Thus $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, implying that it is not a PID or a Euclidean domain.

Ex. 3.32 Let $n \in \mathbb{Z}$. If n is even, we may write $n = 2m$ and thus $n^2 = 4m^2 \equiv 0 \pmod 4$. If n is odd, we may write $n = 2m+1$ and thus $n^2 = (2m+1)^2 = 4m^2 + 4m + 1 \equiv 1 \pmod 4$.

Ex. 3.33 Let π be a prime element in $\mathbb{Z}[i]$ such that $\pi \notin \mathbb{Z}$ and $\pi \notin i\mathbb{Z}$. This means $\pi = x + iy$ where $x, y \neq 0$.

If $N(\pi) = \pi\bar{\pi}$ is even, we may write $\pi\bar{\pi} = 2m = (1+i)(1-i)m$. Now since π is a prime element, we may conclude that π divides $1 \pm i$ or m. If π divides $1 \pm i$, then $N(\pi)$ divides $N(1 \pm i) = 2$, so that $N(\pi) = 2$. If π does not divide any of $1 \pm i$, π divides m, so $m = q\pi$ and $\bar{\pi} = (1+i)(1-i)q$. From Exercise 3.27, $\bar{\pi}$ is also a prime element of $\mathbb{Z}[i]$. As above, we see that if $\bar{\pi}$ divides one of $1 \pm i$, $N(\bar{\pi}) = N(\pi)$ divides 2, so $N(\pi) = 2$. If this is not the case, we may conclude that $\bar{\pi}$ divides q, but then $1 = (1+i)(1-i)r = 2r$ for some $r \in \mathbb{Z}[i]$ which is impossible. Another argument is that $\bar{\pi}$ is irreducible, so one of $1 \pm i$ and q is a unit; thus q is a unit and $\bar{\pi} = 2q$; but then $\bar{\pi}q^{-1} = 2$ which is not a prime element of $\mathbb{Z}[i]$. Altogether we may conclude, that if $N(\pi)$ is even, $N(\pi) = 2$.

Now if $N(\pi)$ is odd, we may write $N(\pi) = \pi\bar{\pi} = p_1 \cdots p_n$ where the p_i are odd primes. Now since π is a prime element, and π divides the right-hand side, there must be some p_i for which $\pi \mid p_i$. But then $N(\pi)$ divides $N(p_i) = p_i^2$. So we see that $N(\pi)$ is either p_i or p_i^2 (1 is impossible, because then π would be a unit). Write $\pi q = p_i$.

Then if $N(\pi) = p_i^2$ then $\pi\bar{\pi} = (\pi q)^2 = \pi^2 q^2$, so $\bar{\pi} = \pi q^2$. Again we use the fact that $\bar{\pi}$ is also a prime element. Clearly $\bar{\pi}$ does not divide π (because both x and y are non-zero); thus $\bar{\pi}$ divides q^2, and hence q. Now this means $\bar{\pi}r = q$ and then $\bar{\pi} = \pi(\bar{\pi}r)^2 = \pi\bar{\pi}^2 r^2$ so $1 = \pi\bar{\pi}r^2$ which is impossible. So we may conclude that $N(\pi) = p_i$. Now by Exercise 32, x^2 and y^2 are congruent to 0 or 1 modulo 4, so their sum $x^2 + y^2 = N(\pi) = p_i$ is congruent to $0, 1$ or 2 modulo 4. Since p_i is odd, $p_i \equiv 1 \pmod 4$.

The prime elements of $\mathbb{Z}[i]$ may now be classified as follows: An element $\pi = x + iy \in \mathbb{Z}[i]$ is a prime element if and only if either

- $xy = 0$ and $|x| + |y|$ is a prime number congruent to 3 modulo 4
- $xy \neq 0$ and $x^2 + y^2 = N(\pi)$ is a prime number congruent to 1 modulo 4 or $x^2 + y^2 = 2$.

First, if π is a prime element, and $xy \neq 0$, we have seen above that $x^2 + y^2$ is a prime which is either 2 or congruent to 1 modulo 4. If π is a prime element with $xy = 0$, we may assume that $\pi = p$ where p is a positive integer, since π is associated to a positive integer. Now clearly p must be a prime. It is not 2, since 2 is not a prime element in $\mathbb{Z}[i]$; thus p is odd. From Corollary 3.5.14, $p \not\equiv 1 \pmod 4$, so $p \equiv 3 \pmod 4$.

Now assume $xy = 0$ and $p = |x| + |y|$ is a prime congruent to 3 modulo 4. Then $\pi = x + iy$ is associated to the prime p; the latter is a prime element of $\mathbb{Z}[i]$ by Lemma 3.5.18, so clearly also π is a prime element.

If $xy \neq 0$ and $x^2 + y^2$ is a prime, then π is a prime element by Proposition 3.5.11. This concludes the classification; determining the prime elements of $\mathbb{Z}[i]$ is therefore just as difficult as finding the primes in $\mathbb{Z}$.

Ex. 3.34 Assume there is only a finite number of primes $\equiv 3 \pmod 4$; list them as $p_1, p_2, \ldots, p_n$. Then the number $N = 4p_1 \cdots p_n - 1$ is clearly larger than any of the p_i, and is congruent to 3 modulo 4. If N is a prime number, we have a contradiction. If N is not a prime number, we may factor it as $N = q_1 \cdots q_k$ where the q_j are primes. Now since N is odd, none of the q_j are 2; ie. they are all odd and thus congruent to either 1 or 3 modulo 4. If they are all congruent to 1 modulo 4, so is their product, which is a contradiction (since N is congruent to 3 modulo 4). Thus at least one of the q_j is congruent to 3 modulo 4. Since $p_1, p_2, \ldots, p_n \nmid N$ this q_j does not already appear in our list of the finitely many primes $\equiv 3 \pmod 4$; thus there are infinitely many such primes.

Ex. 3.35 A little rewriting shows that

$$\begin{aligned} 221 &= 13 \cdot 17 \\ &= (2^2 + 3^2)(1^2 + 4^2) \\ &= N(2 + 3i)N(1 + 4i) \\ &= N((2 + 3i)(1 + 4i)) \\ &= N(-10 + 11i) \\ &= 10^2 + 11^2. \end{aligned}$$

Ex. 3.36 By Exercise 32, the sum of two squares is congruent to either $0, 1$ or 2 modulo 4, and since $51 \equiv 3 \pmod 4$, 51 cannot be written as a sum of two squares.

Ex. 3.37 Let $p = 137$. Then $x = 37$ satisfies $x^2 \equiv -1 \pmod{137}$. Doing the same calculations as in Examples 3.5.16 and 3.5.17 we obtain the table

i	-1	0	1	2	3	4	5	6
r_i	137	37	26	11	4	3	1	0
q_i			3	1	2	2	1	1
a_i	1	0	1	-1	3	-7	10	-17
b_i	0	1	-3	4	-11	26	-37	63

We could of course have stopped after obtaining the remainders $r_2 = 11$ and $r_3 = 4$, since they are the first remainders $< \sqrt{137}$. Now $137 = 11^2 + 4^2$, so the algorithm in fact works in this case.

Ex. 3.38 The points represent the prime elements of $\mathbb{Z}[i]$.

Ex. 3.39 Let p be a prime number. Define

$$\mathbb{Z}_{(p)} = \{\tfrac{a}{s} \in \mathbb{Q} \mid p \nmid s\}.$$

(i) It is quite clear that $\mathbb{Z}_{(p)}$ is in a fact a ring; for if p does not divide s or s', it does not divide ss'; and simple calculations then show that $\mathbb{Z}_{(p)}$ is closed under addition and multiplication and that $0, 1 \in \mathbb{Z}_{(p)}$. Since for every element $a \in \mathbb{Z}$ we have $\frac{a}{1} \in \mathbb{Z}_{(p)}$ (p never divides 1), we have $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$. By definition $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$. Because of the hierarchy $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ we may conclude that $F(\mathbb{Z}) \subseteq F(\mathbb{Z}_{(p)}) \subseteq F(\mathbb{Q})$ where F denotes "field of fractions" and the $\subseteq$ should be read in the sense that there exists an injective ring homomorphism. But $F(\mathbb{Z}) = \mathbb{Q}$ and by Exercise 24 $F(\mathbb{Q}) = \mathbb{Q}$ (they are isomorphic); thus $F(\mathbb{Z}_{(p)}) = \mathbb{Q}$.

(ii) If $u = \frac{a}{s}$ is a unit, $u^{-1} = \frac{s}{a} \in \mathbb{Z}_{(p)}$, so $p \nmid a$. Thus the units $\mathbb{Z}^*_{(p)}$ is the set

$$\{\tfrac{a}{s} \in \mathbb{Q} \mid p \nmid a, p \nmid s\}$$

(iii) Let $x \in \mathbb{Z}_{(p)} \setminus \{0\}$. Then we may write x as $\frac{a}{s}$ where $\gcd(a, s) = 1$. Since $a \neq 0$, there is a largest n such that $p^n \mid a$. Let $a = a'p^n$. Then

$$x = \frac{a}{s} = \frac{a'}{s} p^n$$

and since $p \nmid a'$ we may choose $u = \frac{a'}{s}$. Now assume $x = up^n = u'p^m$, where $u, u' \in \mathbb{Z}_{(p)}$. Then clearly $n = m$, since otherwise p would divide u or u'; and consequently $u = u'$.

(iv) Since I contains at least one non-zero element, it also contains at least one element of the form p^k (since $up^k \in I$ implies $u^{-1}up^k = p^k \in I$). Let $n = \min\{k \in \mathbb{N} \mid p^k \in I\}$. Then since $p^n \in I$ clearly $\langle p^n \rangle \subseteq I$. Let $x \in I$. If $x = 0$ clearly we have $x \in \langle p^n \rangle$. If $x \neq 0$ we have $x = up^k$ for some unit u and some k. Then since $n \leq k$ we have $x = up^{k-n}p^n$, where $up^{k-n} \in \mathbb{Z}_{(p)}$; thus $x \in \langle p^n \rangle$. This shows $I = \langle p^n \rangle$.

(v) From (iv) we may conclude that the only ideals in $\mathbb{Z}_{(p)}$ are $\langle 0 \rangle$ and $\mathbb{Z}_{(p)} \supseteq \langle p \rangle \supseteq \langle p^2 \rangle \supseteq \cdots$. Thus the only maximal ideal is $\langle p \rangle$.

Chapter 4

Ex. 4.1 (i) Let F denote the set of functions from the commutative ring R to itself; $F(R,R)$. Then F is clearly a ring; defining addition and multiplication of functions point-wise as usual. The additive inverse of a function f is $-f$ defined by $(-f)(x) = -f(x)$; the zero element in F is the zero function; ie. the function $x \mapsto 0$ for all $x \in R$; likewise the multiplicative identity in F is the constant function $x \mapsto 1$. The rules of distributivity and commutativity follow from the same properties of R.

(ii) Define $\varphi\colon R[X] \to F$ by $\varphi(a_nX^n + \cdots + a_1X + a_0) = a_nI^n + \cdots + a_1I + a_0$, where I is the identity function $r \mapsto r$. (Strictly speaking, the a_i appearing on the right-hand side should be considered as the constant function $r \mapsto a_i$ in F). Simple calculations show that φ preserves addition and multiplication. The multiplicative neutral element in $R[X]$ is 1, which is mapped to the constant function 1; thus φ is a ring homomorphism.

(iii) If $R = \mathbb{F}_2$, we have for instance $\varphi(0) = 0 = x^2 + x = \varphi(X^2 + X)$; since for all $x \in \mathbb{F}_2$ we have $x^2 = x$ and thus $x^2 + x = x + x = 0$. So the polynomials $X^2 + X$ and the zero polynomial, considered as functions on $\mathbb{F}_2$ are both the zero function, but they are *not* the same polynomial. Thus φ is not necessarily injective.

Assume $R = \mathbb{F}_p$. If $\varphi(P) = 0$, then $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ for all $\alpha \in \mathbb{F}_p$. Then for all $\alpha \in \mathbb{F}_p$ we have $X - \alpha \mid P$, so P must be of the form

$$P = Q \prod_{\alpha \in \mathbb{F}_p} (X - \alpha)^{k_\alpha}$$

where $k_\alpha \geq 1$ and Q is some polynomial over $\mathbb{F}_p[X]$ (with no roots). Clearly, if P is a polynomial on this form, $P(\alpha) = 0$ for every $\alpha \in \mathbb{F}_p$.

Ex. 4.2 (i) Using that two polynomials are the same if and only if they have the same coefficients, we calculate the k'th coefficient of fg.

$$\begin{aligned}(fg)(k) &= \sum_{i+j=k} f(i)g(j)\\ &= \sum_{j+i=k} g(j)f(i)\\ &= (gf)(k)\end{aligned}$$

ie. the k'th coefficient in the polynomial fg is the same as the the k'th coefficient in the polynomial gf (for all k); thus $fg = gf$.

(ii) Again, by looking at the k'th coefficient one sees that

$$\begin{aligned}(f(g+h))(k) &= \sum_{i+j=k} f(i)(g+h)(j) \\ &= \sum_{i+j=k} f(i)[g(j)+h(j)] \\ &= \sum_{i+j=k} f(i)g(j)+f(i)h(j) \\ &= \sum_{i+j=k} f(i)g(j) + \sum_{i+j=k} f(i)h(j) \\ &= (fg)(k)+(fh)(k)\end{aligned}$$

so $f \cdot (g+h) = fg + fh$.

(iii) As above, we will prove that $f(gh) = (fg)h$ by proving that each coefficient is the same. Now

$$\begin{aligned}(f(gh))(k) &= \sum_{i+j=k} f(i)(gh)(j) \\ &= \sum_{i+j=k} f(i) \sum_{r+s=j} g(r)h(s) \\ &= \sum_{\substack{i+j=k \\ r+s=j}} f(i)g(r)h(s) \\ &= \sum_{i+r+s=k} f(i)g(r)h(s) \\ &= \sum_{\substack{j+s=k \\ i+r=j}} f(i)g(r)h(s) \\ &= \sum_{j+s=k} \left(\sum_{i+r=j} f(i)g(r) \right) h(s) \\ &= \sum_{j+s=k} (fg)(j)h(s) \\ &= ((fg)h)(k)\end{aligned}$$

Ex. 4.3 Let $f, g \in R[X] \setminus \{0\}$, with $f+g \neq 0$. We may WLOG assume $\deg f \geq \deg g$. Then $\deg(f+g) \leq \deg(f) = \max(\deg f, \deg g)$, and strict inequality occurs if and only if f and g has the same degree and the leading terms cancel (ie. the leading coefficients sum to 0).

Ex. 4.4 Assume $q \in R[X]$ is a monic polynomial, and that $qp = 0$ for a non-zero polynomial p. Then (viewing q and p as functions $\mathbb{N} \to R$) $(qp)(n) = 0$ for all $n \in \mathbb{N}$; in particular $(qp)(\deg q + \deg p) = 0$. But $(qp)(\deg q + \deg p) = q(\deg q)p(\deg p) = 1p(\deg p) = p(\deg p) = 0$ is impossible, since the leading coefficient of a (non-zero) polynomial cannot be 0. Thus $p = 0$, and q is not a zero divisor after all. If $qf = qg$, $qf - qg = q(f - g) = 0$, so by the above we must have $f - g = 0$; ie. $f = g$.

Ex. 4.5 Assume R is a domain, and let $f, g \in R[X]$ such that $fg = 0$. If both f and g are non-zero polynomials, we would have $(fg)(\deg f + \deg g) = f(\deg f)g(\deg g) \neq 0$, since R is a domain. This contradicts $fg = 0$; thus at least one of f and g must be the zero polynomial.

Ex. 4.6 In $\mathbb{Z}/2\mathbb{Z}$, it is always true that $x^2 - x = [0]$. Thus the polynomial $X^2 - X \in R[X]$ has every element of R (ie. every function $\mathbb{N} \to \mathbb{Z}/2\mathbb{Z}$) as a root, and there are infinitely many such functions.

Ex. 4.7 Assuming there are only finitely many irreducible polynomials $P_1, P_2, \ldots, P_n \in \mathbb{F}_p[X]$, we may form the new polynomial $P = P_1P_2 \cdots P_n + 1$. Either P is an irreducible polynomial, or has an irreducible factorization $P = Q_1Q_2 \cdots Q_k$. Since none of the P_i divides P (they all leave a remainder of 1), all of the Q_i are irreducible polynomials not already on the list of the finitely many; thus there cannot be finitely many irreducible polynomials.

Ex. 4.8 Let R be a UFD and K the field of fractions of R. Assume $\alpha = a/s \in K$, that a and s have no associated prime divisors, and that α is a root in the polynomial

$$a_nX^n + \cdots + a_1X + a_0 \in K[X]$$

where $a_i \in R$.

We immediately see that

$$a_n\frac{a^n}{s^n} + \cdots + a_1\frac{a}{s} + a_0 = 0$$

and, by multiplying both sides with s^n we obtain

$$a_na^n + a_{n-1}a^{n-1}s + \cdots + a_1as^{n-1} + a_0s^n = 0$$

Now we may consider this as an equation only involving elements of R. Moving the first and last term, respectively, to the other side, we see that

$$a_{n-1}a^{n-1}s + \cdots + a_1as^{n-1} + a_0s^n = -a_na^n \tag{4.1}$$

$$a_na^n + a_{n-1}a^{n-1}s + \cdots + a_1as^{n-1} = -a_0s^n \tag{4.2}$$

Now in (4.1), s divides every term on the left-hand side, and thus divides $a_n a^n$. Since s has no prime factors associated to any prime factors of a, s must divide a_n. Similarly in (4.2), a divides every term on the left-hand side, and a has no prime factors in common with s, so a divides a_0.

Now let $\zeta \in \mathbb{R} \setminus \mathbb{Z}$, and assume ζ is a root in the polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, where $a_i \in \mathbb{Z}$. If $\zeta \in \mathbb{Q}$, let $\zeta = a/s$ where a and s are relatively prime. Then from the above we have $a \mid a_0$ and, more interesting, $s \mid 1$. This implies $\zeta \in \mathbb{Z}$ which is a contradiction. Thus ζ is irrational.

Ex. 4.9 Define $D\colon R[X] \to R[X]$ by

$$D(f)(n) = (n+1)f(n+1)$$

ie. $D(f)$ is the function $\mathbb{N} \to R$ which evaluated in n gives $(n+1)f(n+1)$, where as usual the integer $n+1$ should be interpreted as its image under the unique ring homomorphism $\mathbb{Z} \to R$. Using this definition, it is easy to see that

$$\begin{aligned} D(f+g)(n) &= (n+1)(f+g)(n+1) \\ &= (n+1)\big(f(n+1) + g(n+1)\big) \\ &= (n+1)f(n+1) + (n+1)g(n+1) \\ &= D(f)(n) + D(g)(n) \\ &= (D(f) + D(g))(n) \end{aligned}$$

so the polynomials $D(f+g)$ and $D(f)+D(g)$ are in fact the same. In exactly the same way we see that

$$\begin{aligned} D(\lambda f)(n) &= (n+1)(\lambda f)(n+1) \\ &= (n+1)\lambda f(n+1) \qquad (4.3) \\ &= \lambda(n+1)f(n+1) \qquad (4.4) \\ &= \lambda D(f)(n). \end{aligned}$$

At first sight it appears to be necessary that R is commutative to come from (4.3) to (4.4), but it is a fact that if $\varphi\colon \mathbb{Z} \to R$ denotes the unique ring homomorphism, then $\varphi(n)$ commutes with every element of R: Let $x \in \varphi(\mathbb{Z})$ and $y \in R$. Then $x = \varphi(n)$ for some integer n. If n is positive, we may write $xy = (1 + \cdots + 1)y = 1 \cdot y + \cdots + 1 \cdot y = y(1 + \cdots + 1) = yx$. If n is negative, use Exercise III.3 to conclude that $(-1) \cdot y = -y$ and use the above.

Ex. 4.10 The cyclotomic polynomial Φ_p is defined as

$$\Phi_p(X) = \prod_{\substack{1 \le k \le p \\ \gcd(k,p)=1}} (X - e^{2\pi i k/p})$$

and since p is prime, $\gcd(k, p) = 1$ for all $1 \le k < p$. Thus

$$\Phi_p(X) = \prod_{1 \le k < p} (X - e^{2\pi i k/p})$$

Since $X^p - 1 = (X-1)(X^{p-1} + \cdots + X + 1)$, and the roots of the polynomial $X^p - 1$ are all p'th roots of unity, we see that $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ (by removing the factor $X - 1$ corresponding to the only non-primitive p'th root, namely 1).

Ex. 4.11 The above result may be expressed as

$$\Phi_p(X) = \frac{X^p - 1}{X - 1}.$$

Now using the identity

$$X^{p^r} - 1 = \prod_{d \mid p^r} \Phi_d(X)$$

we have

$$\begin{aligned}
\Phi_{p^r}(X) &= \frac{X^{p^r} - 1}{\prod\limits_{\substack{d \mid p^r \\ d < p^r}} \Phi_d(X)} \\
&= \frac{X^{p^r} - 1}{\prod\limits_{d \mid p^{r-1}} \Phi_d(X)} \\
&= \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} \\
&= \Phi_p(X^{p^{r-1}})
\end{aligned}$$

by comparing with the above expression for Φ_p.

Ex. 4.12 This proof is based on induction in n; the base case $n = 3$ is easy:

$$\begin{aligned}
\Phi_6(X) &= X^2 - X + 1 \\
&= (-X)^2 + (-X) + 1 \\
&= \Phi_3(-X).
\end{aligned}$$

The desired is *not* true for $n = 1$, since $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$; so $\Phi_2(-X) = -X + 1 = -(X - 1) = -\Phi_1(-X)$; this observation will be used in the following. Now as usual, consider the identity

$$X^{2n} - 1 = \prod_{d|2n} \Phi_d(X).$$

Then

$$\begin{aligned}
\Phi_{2n}(X) &= \frac{X^{2n} - 1}{\prod\limits_{\substack{d|2n \\ d<2n}} \Phi_d(X)} \\
&= \frac{X^{2n} - 1}{\Phi_n(X)\Phi_1(X)\Phi_2(X) \prod\limits_{\substack{d|n \\ 1<d<n}} \Phi_d(X)\Phi_{2d}(X)} \\
&= \frac{X^{2n} - 1}{-\Phi_n(X)\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(X)\Phi_d(-X)} \\
&= \frac{(X^{2n} - 1)\Phi_n(-X)}{-\Phi_n(X)\Phi_n(-X)\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(X)\Phi_d(-X)} \\
&= \frac{(X^{2n} - 1)\Phi_n(-X)}{-\prod\limits_{d|n} \Phi_d(X)\Phi_d(-X)}
\end{aligned}$$

Now using $\prod\limits_{d|n} \Phi_d(X) = X^n - 1$ and $\prod\limits_{d|n} \Phi_d(-X) = (-X)^n - 1 = -(X^n + 1)$ (since n is odd), we see that the denominator in the last fraction is in fact $-(X^n - 1)(-(X^n + 1)) = (X^n - 1)(X^n + 1) = X^{2n} - 1$, so we may conclude that $\Phi_{2n}(X) = \Phi_n(-X)$.

Ex. 4.13 Let $f = \Phi_8(X) = X^4 + 1$.

(i) Let p be a prime number $\equiv 1 \pmod 4$, and consider f as a polynomial in $\mathbb{F}_p[X]$. By Proposition 1.11.6 (or Lemma 3.5.12) we may find an $\alpha \in \mathbb{F}_p$ such that $\alpha^2 = -1$ (in $\mathbb{F}_p$). Then $f = (X^2 + \alpha)(X^2 - \alpha)$, and f is reducible in $\mathbb{F}_p[X]$.

(ii) Assume $p \equiv 3 \pmod 8$. Then certainly $p \equiv 3 \pmod 4$. From Corollary 1.11.11 we have $\left(\frac{2}{p}\right) = -1$, and from Proposition 1.11.6 we have $\left(\frac{-1}{p}\right) = -1$. Finally from Corollary 1.11.5 we have $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$; thus -2 is a quadratic residue modulo p; or put another way, the congruence $x^2 \equiv -2 \pmod p$ has a solution; put still another way, this means there exist an $a \in \mathbb{F}_p$ with the property that $a^2 = -2$. For this particular a we have

$$\begin{aligned}(X^2 + aX - 1)(X^2 - aX - 1) &= X^4 + (-2 - a^2)X^2 + 1\\ &= X^4 + 1\\ &= f\end{aligned}$$

so f is reducible in $\mathbb{F}_p[X]$.

(iii) Now assume $p \equiv 7 \pmod 8$. Then as above we may use Corollary 1.1.11; this time to conclude that 2 is a quadratic residue modulo p; thus there is an $a \in \mathbb{F}_p$ with $a^2 = 2$. Then calculation yields

$$\begin{aligned}(X^2 + aX + 1)(X^2 - aX + 1) &= X^4 + (2 - a^2)X^2 + 1\\ &= X^4 + 1\\ &= f\end{aligned}$$

so f is again reducible in $\mathbb{F}_p[X]$.

(iv) Since every odd prime is either congruent to 3 or 7 modulo 8 or congruent to 1 modulo 4, it follows that f is reducible in $\mathbb{F}_p[X]$ for every odd prime. In $\mathbb{F}_2[X]$ we have the identity $X^4 + 1 = (X + 1)^4$, so f is certainly reducible in $\mathbb{F}_2[X]$. Thus f is reducible in $\mathbb{F}_p[X]$ for every prime p.

Ex. 4.14 Let $n \in \mathbb{N}$, $n > 1$.

(i) The set of n'th roots of unity is $C_n = \{e^{2\pi ik/n} \mid k = 0, \dots, n-1\}$. It is quite clear that $C_n = \langle e^{2\pi i/n}\rangle$ (as a multiplicative group), and since C_n has order n, it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ (an example of an isomorphism is $e^{2\pi ik/n} \mapsto [k]$).

(ii) The elements of order n in C_n are exactly the primitive n'th roots of unity, and since (Lemma 4.4.1) an element $e^{2\pi ik/n} \in C_n$ is a primitive n'th root if and only if $\gcd(k, n) = 1$, there are exactly $\varphi(n)$ such primitive roots; since C_n and $\mathbb{Z}/n\mathbb{Z}$ are isomorphic, there are also $\varphi(n)$ elements of order n in the latter.

Ex. 4.15 Let $\varphi\colon R \to S$ be a ring homomorphism. Define $\varphi'\colon R[X] \to S[X]$ by

$$\varphi'(a_nX^n + \ldots a_1X + a_0) = \varphi(a_n)X^n + \cdots + \varphi(a_1)X + \varphi(a_0)$$

Let P and Q be polynomials in $R[X]$. For notational convenience I will write $P = a_nX^n + \ldots a_1X + a_0$ and $Q = b_nX^n + \cdots + b_1X + b_0$, even if P and Q does not have the same degree (just add some 0-coefficients). Then

$$\begin{aligned}\varphi'(P+Q) &= \varphi'((a_n+b_n)X^n + \cdots + (a_1+b_1)X + a_0 + b_0)\\ &= \varphi(a_n+b_n)X^n + \cdots + \varphi(a_1+b_1)X + \varphi(a_0+b_0)\\ &= \varphi(a_n)X^n + \varphi(b_n)X^n + \cdots + \varphi(a_1)X + \varphi(b_1)X + \varphi(a_0) + \varphi(b_0)\\ &= \varphi'(P) + \varphi'(Q)\end{aligned}$$

A similar argument will show that $\varphi'(PQ) = \varphi'(P)\varphi'(Q)$, although the simplicity of the argument will probably drown in the notation. The remaining few criteria for φ' being a ring homomorphism are also easily checked.

Ex. 4.16 Let R be a domain, and let G be a finite subgroup of $(R^*, \cdot)$. Let $N = |G|$. The polynomial

$$X^N - 1 = \prod_{d|N} \Phi_d(X)$$

may be viewed as an element in $R[X]$. Every element in G is a root in this polynomial, since the order of each element divides N; so $\alpha^N = 1$ for every $\alpha \in G$. Since (Proposition 4.3.5) the polynomial can have no more than N roots, all roots of the polynomial are elements of G. Consider the right-hand side representation; it contains $\Phi_N(X)$ as a factor. Thus all primitive N'th roots of unity are elements in G, and since each of these generate a (cyclic) subgroup of G of order N, this subgroup must be G itself. Thus G is cyclic.

Ex. 4.17 By trial and error one finds that $\mathbb{F}_{17}^*$ is generated by 3; since

$$\langle 3\rangle = \{3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1\}.$$

Ex. 4.18 If G is a finite subgroup of $\mathbb{C}^*$, every element of G must lie on the unit circle; if this was not the case, let $\alpha \in G$ be an element with $|\alpha| \neq 1$. Then $\alpha, \alpha^2, \ldots$ is an infinite sequence, where no element is ever repeated, and since $\langle\alpha\rangle \subseteq G$, G would be infinite. Let $N = |G|$. For every element α_i we may choose a real number $0 \leq t_i < N$ such that

$$\alpha_i = e^{2\pi i t_i/N}$$

Let t denote the least of the t_i larger than 0, and let $\alpha = e^{2\pi i t/N}$. The claim is that α generates G. If $\operatorname{ord}\alpha < N$, we may choose an element β in G outside of $\langle\alpha\rangle$. Consider the elements $\beta, \beta\alpha, \beta\alpha^2, \dots, \beta\alpha^{\operatorname{ord}\alpha-1}$. Because multiplication with α^n corresponds to a rotation of $\frac{2\pi tn}{N}$, at least one of these "lies between" 1 and α on the unit circle, contrary to the choice of α. Thus no such β can exist, and $\operatorname{ord}\alpha = N$; that is, G is cyclic.

Ex. 4.19 Assume $\mathbb{R}^*$ is a cyclic group; say $\mathbb{R}^* = \langle a\rangle$. Clearly we must have $|a| \neq 1$. We may WLOG assume that $|a| > 1$ (a is a generator if and only if a^{-1} is a generator). Choose any real number x in the interval (a^2, a^4), different from α^3. This is clearly a unit, since $x > 0$. But x cannot be an integer power of a, which one may see simply by observing that $|a^n| > a^4 > x$ for $n > 4$ and $|a^n| < a^2 < x$ for $n < 2$; ie. $\langle a\rangle \subsetneq \mathbb{R}^*$. One may also argue that any cyclic group is countable, but the set of real numbers is uncountable (and so is the set of real numbers with 0 excluded!), so $\mathbb{R}^*$ cannot even be finitely generated (since $\mathbb{Z}^n$ is countable for all n). Also it cannot be countably generated.

Ex. 4.20 Assume p is a prime number. Then since $\mathbb{F}_p$ is a field, the group of units $\mathbb{F}_p^*$ is a cyclic group (of order $\varphi(p) = p-1$). Let $[a]$ be a generator for this group. Then clearly $a^{p-1} \equiv 1 \pmod p$, because the order of $[a]$ is $p-1$. For this very same reason, for every prime q dividing $p-1$, we have $a^{(p-1)/q} \not\equiv 1 \pmod p$.

Now assume there is an integer a with the given properties. Then $[a]$ is a unit in $\mathbb{Z}/p\mathbb{Z}$, and the order of $[a]$ in $\mathbb{Z}/p\mathbb{Z}^*$ divides $p-1$. But since $a^{(p-1)/q} \not\equiv 1 \pmod p$ for every q dividing $p-1$, the order of a in $\mathbb{Z}/p\mathbb{Z}^*$ must be $p-1$. This means in particular that there are $p-1$ units in $\mathbb{Z}/p\mathbb{Z}$; thus $\mathbb{Z}/p\mathbb{Z}$ is a field, and p is a prime number (Proposition 3.2.3).

Ex. 4.21 Let p be an odd prime, $a \in \mathbb{N}$ a primitive root modulo p, and $G = (\mathbb{Z}/p^2\mathbb{Z})^*$.

(i) The order of G is $\varphi(p^2) = p^2 - p = p(p-1)$; thus $\operatorname{ord}_G([a]) \mid p(p-1)$. On the other hand we have by definition

$$a^{\operatorname{ord}_G([a])} \equiv 1 \pmod{p^2}$$

so $a^{\operatorname{ord}_G([a])} \equiv 1 \pmod p$. Put another way, $a^{\operatorname{ord}_G([a])} = 1 \in \mathbb{F}_p^*$, but then $\operatorname{ord}_{\mathbb{F}_p^*}([a]) = p-1 \mid \operatorname{ord}_G([a])$. Now the only possible values for $\operatorname{ord}_G([a])$ are $p-1$ and $p(p-1)$.

(ii) Suppose $a^{p-1} \equiv 1 \pmod{p^2}$. Let $r = a+p$. Then the binomial formula gives

$$\begin{aligned} r^{p-1} &= (a+p)^{p-1} \\ &= \sum_{i=0}^{p-1} \binom{p-1}{i} a^{p-1-i} p^i \\ &\equiv a^{p-1} + (p-1)a^{p-2}p \\ &\equiv 1 - pa^{p-2} \pmod{p^2} \end{aligned}$$

Then $r^{p-1} \not\equiv 1 \pmod{p^2}$ (because otherwise $p^2 \mid pa^{p-2}$ implying $p \mid a$ which is impossible). It also follows from the above that p divides $r^{p-1} - 1$, so $r^{p-1} = 1 + tp$, where $p \nmid t$.

(iii) Assume $\text{ord}_G([a]) = p - 1$. Since a and $a + p$ are the same in $\mathbb{F}_p$, they are both primitive roots modulo p. Then from (i) we may conclude that $\text{ord}_G([a + p])$ is either $p - 1$ or $p(p - 1)$. Now from (ii) we know that $(a + p)^{p-1} \not\equiv 1 \pmod{p^2}$, so we must have $\text{ord}_G([a + p]) = p(p - 1)$.

(iv) First of all, we need to assure the existence of a primitive root modulo p; since $\mathbb{F}_p$ is a field $\mathbb{F}_p^*$ is cyclic, so there does in fact exist an a with the desired property. Now if $\text{ord}_G([a]) = p(p - 1)$ we are done, because then $[a]$ generates G. If not, it follows from (i) that $\text{ord}_G([a]) = p - 1$, so from (iii) $[a + p]$ generates G. Thus $(\mathbb{Z}/p^2\mathbb{Z})^*$ is cyclic.

(v) Suppose $a^{p-1} = 1 + tp$ where $p \nmid t$. By raising both sides to p^{m-1} we get

$$\begin{aligned} a^{p^{m-1}(p-1)} &= (1+tp)^{p^{m-1}} \\ &= \sum_{i=0}^{p^{m-1}} \binom{p^{m-1}}{i} t^i p^i \\ &= 1 + tp^m + \sum_{i=2}^{p^{m-1}} \binom{p^{m-1}}{i} t^i p^i \end{aligned}$$

Now since $n \mid \binom{n}{i}$ for $1 \leq i \leq n - 1$ we see that p^{m+1} divides all terms of the sum; with the possible exception of the last. The last term contains the factor $p^{p^{m-1}}$. Since $m + 1 \leq p^{m-1}$ for $m > 1$ and $p \geq 3$ (use $3^{m-1} \leq p^{m-1}$ and show $m + 1 \leq 3^{m-1}$), p^{m+1} also divides the last term. Clearly then p^m divides all terms but the very first, 1, so we may write

$$a^{p^{m-1}(p-1)} = 1 + t_m p^m$$

and since p^{m+1} does not divide the term tp^m, $p \nmid t_m$.

(vi) Let $a \in \mathbb{N}$ have the following properties: $[a]_p$ generates $(\mathbb{Z}/p\mathbb{Z})^*$ and $[a]_{p^2}$ generates $(\mathbb{Z}/p^2\mathbb{Z})^*$; furthermore $a^{p-1} = 1 + tp$ where $p \nmid t$. Such an a must exist; choose any generator for $(\mathbb{Z}/p\mathbb{Z})^*$; if it also generates $(\mathbb{Z}/p^2\mathbb{Z})^*$ we are done, because then $a^{p-1} \not\equiv 1 \pmod{p^2}$; if not, add p to this generator, then by (ii) we have an a which satisfies the given properties.

Now $a^{p^{m-1}(p-1)} = 1+t_m p^m$ for all $m \geq 1$. The claim is that $[a]$ generates $G_m = (\mathbb{Z}/p^m\mathbb{Z})^*$ for all $m \geq 1$. Let $m \geq 3$. Now since $a^{\operatorname{ord}_{G_m}(a)} \equiv 1 \pmod{p^m}$, we certainly have $a^{\operatorname{ord}_{G_m}(a)} \equiv 1 \pmod{p}$, implying $p - 1 \mid \operatorname{ord}_{G_m}(a)$. Furthermore, $\operatorname{ord}_{G_m}(a) \mid |G_m| = p^{m-1}(p-1)$.

Now assume $\operatorname{ord}_{G_m}(a) < p^{m-1}(p-1)$. Then we must have $a^{p^{m-2}(p-1)} \equiv 1 \pmod{p^m}$. But this is impossible, since $a^{p^{m-2}(p-1)} = 1 + t_{m-1}p^{m-1}$ and $p \nmid t_{m-1}$. Thus $\operatorname{ord}_{G_m}(a) = p^{m-1}(p-1)$, ie. $(\mathbb{Z}/p^m\mathbb{Z})^*$ is generated by $[a]$ and is therefore cyclic.

Ex. 4.22 Let p be an odd prime, and let a be a primitive root modulo p. Let $x = a^{(p-1)/2}$. Then $x \not\equiv 1 \pmod{p}$, since a is a primitive root. But $x^2 = a^{p-1} \equiv 1 \pmod{p}$, so $p \mid x^2 - 1 = (x+1)(x-1)$; ie. $x + 1 \equiv 0 \pmod{p}$ or $x - 1 \equiv 0 \pmod{p}$. This implies $x \equiv -1 \pmod{p}$.

Ex. 4.23 Let p be a prime number.

(i) Suppose p divides $10^s - 1$, where $s \in \mathbb{N}$ ($s \neq 0$). Then for some $0 \leq x < 10^s$ we have $px = 10^s - 1$, which we may rewrite as

$$\begin{aligned} px &= 10^s - 1 \\ x + \frac{1}{p} &= \frac{10^s}{p} \\ \frac{1}{p} &= \frac{x}{10^s} + \frac{1}{10^s}\frac{1}{p} \end{aligned}$$

Thus the decimals in $1/p$ must begin repeating after at most s digits, and the period can not be longer than s.

(ii) The period of p can clearly not be longer than $p - 1$, since there only $p - 1$ different possible remainders (excluding 0, which would imply a finite decimal expansion) in each step of the division algorithm, and as soon as one of these reappears, the algorithm cycles.

(iii) Assume p is different from 2 and 5, so that $[10]$ is in fact a unit in $\mathbb{Z}/p\mathbb{Z}$. The period is the number of steps in the division algorithm performed between two repetitions. But "a step" in the division algorithm is exactly multiplying the previous remainder by 10 and counting how many times p divides the result; leaving a new remainder. The first "remainder" in $1/p$ is 1, so the first repetition is when 1 is again encountered; this happens exactly after $\operatorname{ord}_p([10])$ steps.

Ex. 4.24 Let p be an odd prime, and let $\alpha = [X] \in R = \mathbb{F}_p[X]/\langle X^4 + 1\rangle$.

(i) From Proposition 4.6.7, we may write elements of R uniquely as polynomials of degree ≤ 3 in α. Then clearly $\alpha^k \neq 1$ for $k = 1, 2, 3$. Using $\alpha^4 = -1$ we obtain

$$\begin{aligned}\alpha^4 &= -1\\ \alpha^5 &= -\alpha\\ \alpha^6 &= -\alpha^2\\ \alpha^7 &= -\alpha^3\\ \alpha^8 &= -\alpha^4 = 1\end{aligned}$$

Notice that $-1 \neq 1$ since p is an odd prime. Thus α is a primitive 8'th root.

(ii) Let $y = \alpha + \alpha^{-1}$. A little calculation shows

$$\begin{aligned}\alpha^{-1} &= \alpha^7\\ &= \alpha^3 \cdot \alpha^4\\ &= -\alpha^3\end{aligned}$$

so that $y^2 = (\alpha - \alpha^3)^2 = \alpha^2 + \alpha^6 - 2(-\alpha^4) = \alpha^2 - \alpha^2 + 2 = 2$.

Since clearly $\operatorname{char} R = p$, it follows from Theorem 3.3.9 ("Freshman's Dream") that $y^p = \alpha^p + \alpha^{-p}$.

(iii) Assume $p \equiv \pm 1 \pmod 8$. Then $p = 8m \pm 1$ for some m. Then

$$\begin{aligned}y^p &= \alpha^p + \alpha^{-p}\\ &= \alpha^{8m\pm 1} + \alpha^{-8m\mp 1}\\ &= \alpha^{\pm 1} + \alpha^{\mp 1}\\ &= y\end{aligned}$$

Now assume $p \equiv \pm 3 \pmod 8$. Then $p = 8m \pm 3$, and

$$\begin{aligned} y^p &= \alpha^p + \alpha^{-p} \\ &= \alpha^{8m\pm 3} + \alpha^{-8m\mp 3} \\ &= \alpha^{\pm 3} + \alpha^{\mp 3} \\ &= \alpha^3 + \alpha^{-3} \\ &= -\alpha^{-1} - \alpha^1 \\ &= -y \end{aligned}$$

where the fact $\alpha^4 = \alpha^{-4} = -1$ was used.

(iv) For any odd prime p, we know that the $y \in R$ defined above satisfies $y^2 = 2$. Using the natural mappings $\mathbb{Z} \to \mathbb{F}_p \to \mathbb{F}_p[X] \to R$ it makes sense to consider $\left(\frac{2}{p}\right)$ as an element in R. Since R has characteristic p, we have by Theorem 1.11.4 that

$$\begin{aligned} \left(\frac{2}{p}\right) &= 2^{(p-1)/2} \\ &= (y^2)^{(p-1)/2} \\ &= y^{p-1} \\ &= \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases} \end{aligned}$$

by (iii). Although this identity is obtained using properties of R, it is clear that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

also holds when considered as an identity in $\mathbb{Z}$ (because we know that $\left(\frac{2}{p}\right)$ is either 1 or -1 in $\mathbb{Z}$, and since p is odd, $1 \neq -1$ in R).

Ex. 4.25 Define $a_{-1} = b_0 = 1$ and $a_0 = b_{-1} = 0$. Letting $r_{-1} = X^7 + X^6 + X^2 + X + 1$ and $r_0 = X^7 + X^5 + X^4 + X^2 + 1$, the q_i, r_i, a_i, b_i in Figure 4 may be computed. Thus

$$\begin{aligned} &\gcd(X^7 + X^6 + X^2 + X + 1, X^7 + X^5 + X^4 + X^2 + 1) \\ &\quad = X^3 + X^2 + 1 \\ &\quad = (X^3 + X + 1)(X^7 + X^6 + X^2 + X + 1) \\ &\qquad + (X^3 + X^2)(X^7 + X^5 + X^4 + X^2 + 1) \end{aligned}$$

$$
\begin{array}{ll}
q_1 = 1 & a_1 = a_{-1} - q_1 a_0 = 1 \\
r_1 = r_{-1} - q_1 r_0 = X^6 + X^5 + X^4 + X & b_1 = b_{-1} - q_1 b_0 = -1 = 1 \\
q_2 = X + 1 & a_2 = a_0 - q_2 a_1 = X + 1 \\
r_2 = r_0 - q_2 r_1 = X^5 + X + 1 & b_2 = b_0 - q_2 b_1 = X \\
q_3 = X + 1 & a_3 = a_1 - q_3 a_2 = X^2 \\
r_3 = r_1 - q_3 r_2 = X^4 + X^2 + X + 1 & b_3 = b_1 - q_3 b_2 = X^2 + X + 1 \\
q_4 = X & a_4 = a_2 - q_4 a_3 = X^3 + X + 1 \\
r_4 = r_2 - q_4 r_3 = X^3 + X^2 + 1 & b_4 = b_2 - q_4 b_3 = X^3 + X^2 \\
q_5 = X + 1 & \\
r_5 = r_3 - q_5 r_4 = 0 &
\end{array}
$$

Figure 4: A long list of quotients and remainders…

Ex. 4.26 Let $R = \mathbb{F}_3[X]$.

(i) There are $3^2 = 9$ monic polynomials of degree 2 in R. Of these, 3 have 0 as constant term, so 0 is a root, and they are therefore reducible. The remaining 6 are

$$
\begin{aligned}
&X^2 + X + 1 \\
&X^2 + 2X + 1 \\
&X^2 + 2 \\
&X^2 + 1 \\
&X^2 + 2X + 2 \\
&X^2 + X + 2
\end{aligned}
$$

The first three of these have roots ($\{1\}$, $\{2\}$, $\{1, 2\}$, respectively), whereas the last three are easily seen to have no roots. Thus by Proposition 4.6.3 they are irreducible, and the only such polynomials.

(ii) Assume $f \in R$ is a polynomial of degree 5 with no roots (ie. no polynomial of degree 1 divides f). Then if f is reducible, we may factor it as $f = gh$, where $\deg g + \deg h = \deg f = 5$, but since $\deg g, \deg h > 1$, we must have $\deg g = 2$ and $\deg h = 3$ (or the symmetric case). We may clearly choose g to be monic (since $\mathbb{F}_3$ is a field), and g cannot have any roots, since this would mean f had a root.

(iii) Let $f = X^5 - X + 1$. Then f is polynomial of degree 5 with no roots (since $f(0) = f(1) = f(2) = 1$). If f is reducible, by (ii) we must have a monic irreducible polynomial of degree 2 dividing f. From (i), there are only three such polynomials, and whether they divide f is checked using the division algorithm:

$$\begin{array}{llll}
X^5 - X + 1 & : & X^2 + 1 & = X^3 - X \\
\underline{X^5 + X^3} & & & \\
-X^3 - X + 1 & & & \\
\underline{-X^3 - X} & & & \\
1 \neq 0 & & &
\end{array}$$

$$\begin{array}{llll}
X^5 - X + 1 & : & X^2 + 2X + 2 & = X^3 + X^2 + 2X \\
\underline{X^5 + 2X^4 + 2X^3} & & & \\
X^4 + X^3 - X + 1 & & & \\
\underline{X^4 + 2X^3 + 2X^2} & & & \\
2X^3 + X^2 - X + 1 & & & \\
\underline{2X^3 + X^2 + X} & & & \\
X + 1 \neq 0 & & &
\end{array}$$

$$\begin{array}{llll}
X^5 - X + 1 & : & X^2 + X + 2 & = X^3 - X^2 + 2X \\
\underline{X^5 + X^4 + 2X^3} & & & \\
-X^4 + X^3 - X + 1 & & & \\
\underline{-X^4 - X^3 - 2X^2} & & & \\
2X^3 + 2X^2 - X + 1 & & & \\
\underline{2X^3 + 2X^2 + X} & & & \\
X + 1 \neq 0 & & &
\end{array}$$

Since none of the irreducible monic polynomials of degree 2 divide f, we may conclude that f is not reducible; ie. f is irreducible. Then $\langle f \rangle$ is a maximal ideal, and $L = R/\langle f \rangle$ is a field (Proposition 4.6.3). The number of elements in L may be found using Proposition 4.6.7. Since every element in L may be written uniquely as $[b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4]$ where $b_i \in \mathbb{F}_3$, there are exactly $3^5 = 243$ elements in L.

Let $\alpha = [X] \in L$. Then since $1 = -\alpha^5 + \alpha$, we see that $\gamma = -\alpha^4 + 1$ satisfies $\alpha\gamma = 1$.

Ex. 4.27 Assume $f \in \mathbb{C}[X]$ is an irreducible polynomial. Then f cannot have degree ≥ 2, since then f would have roots (the fundamental theorem of algebra asserts that every non-constant polynomial with complex coefficients has at least one root). Clearly, $\deg f$ cannot be 0, since f would then be a unit in $\mathbb{C}[X]$, which by definition is not irreducible (nor is it reducible). If $\deg f$ is not defined, $f = 0$, and we may write $f = 0 \cdot (X)$; thus $f = ab$ does not imply that a or b is a unit, so 0 is not irreducible. This means we must have $\deg f = 1$.

Ex. 4.28 Let $R = \mathbb{F}_2[X]$.

(i) The polynomial $f = X^5 + X + 1$ clearly has no roots in $\mathbb{F}_2$. Thus to show that the polynomial is reducible, we must find a polynomial of degree 2 dividing f. This second-degree polynomial cannot have any roots (if it had, it could not divide f), so the only possibility is $X^2 + X + 1$. A few calculations shows that this does in fact divide f, and that $f = (X^2 + X + 1)(X^3 + X^2 + 1)$. Thus f is not irreducible.

(ii) Let $g = X^4 + X + 1$. Since g has no roots in $\mathbb{F}_2$, the only way g may factor non-trivially is as $g = ab$, where a and b are second-degree, irreducible polynomials. This is only possible if $X^2 + X + 1$ divides g, and since this is not the case, g is irreducible.

(iii) It follows from Proposition 4.6.3 that $L = R/\langle X^4 + X + 1\rangle$ is a field. The number of elements is $2^4 = 16$, which may be seen from Proposition 4.6.7.

(iv) Since L is a finite field, L^* is a finite group; since L^* may be considered as a subgroup of itself, it is cyclic (Theorem 4.5.3). Since $|L| = 16$, $|L^*| = 15$, and $\operatorname{ord} \alpha \mid 15$. One finds

$$\begin{aligned} \alpha^4 &= \alpha + 1 \\ \alpha^5 &= \alpha^2 + \alpha \end{aligned}$$

Thus since $\alpha, \alpha^3, \alpha^5 \neq 1$, we must have $\operatorname{ord} \alpha = 15$, so α generates L^*.

Ex. 4.29 Let $L = \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$.

(i) Since $X^3 + X + 1$ is irreducible in $\mathbb{F}_2[X]$ (it has no roots, Proposition 4.6.3), L is a field, and the usual counting argument (Proposition 4.6.7) gives that $|L| = 2^3 = 8$.

(ii) The 7 elements of L^* are ($\alpha = [X]$)

$$1, 1+\alpha, 1+\alpha^2, 1+\alpha+\alpha^2, \alpha, \alpha+\alpha^2, \alpha^2$$

By repeated us of the rules $\alpha^3 + \alpha + 1 = 2 = 0 \in L$ one may calculate

$$\begin{aligned}\prod_{x \in L^*} x &= 1(1+\alpha)(1+\alpha^2)(1+\alpha+\alpha^2)(\alpha)(\alpha+\alpha^2)(\alpha^2)\\ &= (1+\alpha+\alpha^2+\alpha^3)(1+\alpha+\alpha^2)(\alpha)(\alpha+\alpha^2)(\alpha^2)\\ &= \alpha^5(1+\alpha+\alpha^2)(\alpha+\alpha^2)\\ &= \alpha^6(\alpha+2\alpha^2)\\ &= \alpha^7\\ &= \alpha^3\alpha^3\alpha\\ &= (-\alpha-1)(-\alpha-1)\alpha\\ &= \alpha(\alpha+1)^2\\ &= \alpha^3+2\alpha^2+\alpha\\ &= -1\end{aligned}$$

(iii) Let K be a finite field with N elements. Then N is of the form p^n, where p is a prime and $n \geq 1$. From §4.8.2 we have

$$X^N - X = \prod_{a \in K} X - a$$

and by canceling the factor X (corresponding to $a = 0$) from both sides we see that

$$X^{N-1} - 1 = \prod_{a \in K^*} X - a$$

so $X^{N-1} - 1$ is a product of $|K^*| = N - 1$ polynomials of degree 1 with non-zero constant coefficient.

(iv) It follows from (iii) by comparing constant terms that

$$-1 = \prod_{a \in K^*} -a$$

and by extracting the $-$ from each factor on the right-hand side, we see that

$$-1 = (-1)^{N-1} \prod_{a \in K^*} a$$

which is the same as

$$(-1)^N = \prod_{a \in K^*} a$$

Now if N is odd, $(-1)^N = -1$ and the desired result follows. If N is even, $\operatorname{char} K = p = 2$, so that $-1 = 1$.

Ex. 4.30 Let $R = \mathbb{F}_2[X]/\langle X^3 + 1\rangle$ and $\alpha = [X] \in R$.

(i) Clearly $(X^2 + X + 1)(X + 1) = X^3 + 1$. Both factors are irreducible; the former because it is a second-degree polynomial with no roots, the latter because it has degree 1 (Proposition 4.6.3).

(ii) From Proposition 4.6.7, we may write every element of R uniquely as $b_0 + b_1\alpha + b_2\alpha^2$, where $b_i \in \mathbb{F}_2$. Thus there must be $|R| = 2^3 = 8$ elements in R.

Since $[X^3 + 1] = \alpha^3 + 1 = 0 \in R$ we see

$$\begin{aligned}(\alpha^2 + \alpha + 1)(\alpha + 1) &= \alpha^3 + \alpha^2 + \alpha + \alpha^2 + \alpha + 1) \\ &= \alpha^3 + 1 \\ &= 0\end{aligned}$$

(iii) Since $(\alpha^2 + \alpha + 1)(\alpha + 1) = \alpha^3 + 1 = 0 \in R$, and none of the factors are 0, both factors are zero divisors, and therefore (by Exercise 3.1) they are not units. Then also $\alpha^2 + \alpha = \alpha(\alpha + 1)$ and $\alpha^2 + 1 = (\alpha + 1)(\alpha + 1)$ are zero divisors, so they are not units.

(iv) The only remaining possible units in R are α, α^2 and of course 1. These are in fact units, since $\alpha \cdot \alpha^2 = \alpha^3 = 1$, and we also see that $R^* = \langle\alpha\rangle$.

Ex. 4.31 Let $R = \mathbb{F}_2[X]$.

(i) There are 4 polynomials of degree 2 in R. Since $X^2, X^2 + 1$ and $X^2 + X$ all factor non-trivially $(X \cdot X, (X + 1)^2, X(X + 1))$ they are reducible. The last polynomial, $X^2 + X + 1$ has no roots in $\mathbb{F}_2$ and is irreducible (Proposition 4.6.3).

(ii) By a similar argument as above, one finds that of the 8 polynomials of degree 3 in R, 4 has 0 as constant coefficient, and therefore 0 as a root. Of the remaining, $X^3 + X^2 + X + 1$ and $X^3 + 1$ both have 1 as a root. Since $X^3 + X^2 + 1$ and $X^3 + X + 1$ have no roots, they are irreducible.

(iii) An irreducible polynomial of degree 6 must have non-zero constant coefficient, and it must have an odd number of non-zero terms (otherwise 1 would be a root). The polynomials $f = X^6 + X + 1$ and $g = X^6 + X^5 + 1$ satisfy these criteria, and one may show that f and g are not divisible by any of the above mentioned irreducible second- and third-degree irreducible polynomials. Thus no polynomial of degree $1, 2$ or 3 divides f or g, and they are irreducible.

(iv) Since f and g are irreducible, $R/\langle f\rangle$ and $R/\langle g\rangle$ are fields; they must have the same number of elements ($2^6 = 64$), and finite fields with the same number of elements are isomorphic (§4.8.2).

Ex. 4.32 Let $R = \mathbb{F}_2[X]$.

(i) In all polynomial rings we have $X - 1 \mid X^n - 1$ for all $n \geq 1$, since $(X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1) = X^n - 1$. Thus in particular $X - 1 \mid X^7 - 1 \in R$. The quotient $f = (X^7 - 1)/(X - 1)$ is then clearly $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$. The ring $R/\langle f\rangle$ contains $2^6 = 64$ elements by Proposition 4.6.7.

(ii) The irreducible polynomials in R of degree 3 are $X^3 + X + 1$ and $X^3 + X^2 + 1$ (see Exercise 31(ii)). One finds that

$$f = (X^3 + X^2 + 1)(X^3 + X + 1).$$

(iii) $R/\langle f\rangle$ is not a field, since it contains zero divisors; for instance $[X^3 + X^2 + 1] \cdot [X^3 + X + 1] = [f] = 0$; or equivalently f is not irreducible.

Ex. 4.33 A field with 8 elements is the field L from Exercise 29; $L = \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$.

Ex. 4.34 Consider the field $\mathbb{F}_{p^n}$, where as usual p is a prime and $n \geq 1$, and let R denote the polynomial ring $\mathbb{F}_{p^n}[X]$, which is clearly a domain. Then the field of fractions for this ring is infinite (since it contains R as a subring), but the characteristic is still p.

Ex. 4.35 As usual, when finding irreducible polynomials of degree 3, the only thing to make sure is that there are no roots. In particular the constant coefficient must not be 0. There are then $3 \cdot 3 \cdot 2 = 18$ possible irreducible monic polynomials of degree 3. Let $f = X^3 + aX^2 + bX + c$. Then f is irreducible if and only if $f(0), f(1), f(2) \neq 0$, that is,

$$\begin{aligned} c &\neq 0 \\ 1 + a + b + c &\neq 0 \\ 2 + a + 2b + c &\neq 0 \end{aligned}$$

If $c \neq 0$, then $c = 1$ or $c = 2$, which gives the following two systems

$$\begin{aligned} a+b &\neq 1 \\ a+2b &\neq 0 \end{aligned} \qquad\qquad \begin{aligned} a+b &\neq 0 \\ a+2b &\neq 2 \end{aligned}$$

From these inequations[4], one finds that the irreducible polynomials are

$$\begin{aligned} &X^3+2X+1 \\ &X^3+X^2+2X+1 \\ &X^3+2X^2+1 \\ &X^3+2X^2+X+1 \\ &X^3+2X+2 \\ &X^3+X^2+2 \\ &X^3+X^2+X+2 \\ &X^3+2X^2+2X+2 \end{aligned}$$

Ex. 4.36 As above, a monic irreducible polynomial of degree 4 is of the form $X^4 + aX^3 + bX^2 + cX + 1$, where $a+b+c \neq 0$; ie. either one of a, b, c is equal to 1 (the others being 0), or they are all three equal to 1. The polynomial X^4+X^2+1 factors as $(X^2+X+1)^2$, so it is not irreducible, but the remaining three,

$$\begin{aligned} &X^4+X^3+X^2+X+1 \\ &X^4+X^3+1 \\ &X^4+X+1 \end{aligned}$$

are in fact irreducible, since they have no roots in $\mathbb{F}_2$ and no irreducible factor of degree 2 (the only such candidate would be X^2+X+1).

Ex. 4.37 The four axioms of Definition B.0.9 are easily seen to be satisfied for the pair (F, R) where $F \subseteq R$. (i) is true because multiplication is associative in R. (ii) is true because the identity element $1 \in F$ is also the identity element in R. (iii) and (iv) are true because multiplication is distributive over addition in R.

Ex. 4.38 (i) If K is a field with p^n elements, and L is a subfield with p^m elements, then L^* is a subgroup of K^*, which means that $p^m - 1 \mid p^n - 1$. From Lemma 4.8.3 we then have $m \mid n$.

[4] This is the best word I could find for it; take a look at `http://mathworld.wolfram.com/Inequation.html`

(ii) If $r \mid s$, then $p^r - 1 \mid p^s - 1$. Then since

$$X^{p^r} - X = X \prod_{d \mid p^r - 1} \Phi_d(X)$$
$$X^{p^s} - X = X \prod_{d \mid p^s - 1} \Phi_d(X)$$

and since all divisors in $p^r - 1$ are also divisors in $p^s - 1$, the former polynomial divides the latter.

(iii) Let $L = \{x \in K \mid x^{p^m} = x\}$. Then for $x, y \in L$ we have $x + y = x^{p^m} + y^{p^m} = (x+y)^{p^m}$, so $x + y \in L$ since $\operatorname{char} K = p$. Clearly $0 \in L$. If $x \in L$, then $-x = -(x^{p^m}) = (-x)^{p^m}$ if p is odd; if $p = 2$ we have $-x = x$; in either case $-x \in L$.

It is easily seen that if $x, y \in L$ then $xy \in L$, and clearly $1 \in L$. Now if $x \in L \setminus \{0\}$, we have $x^{-1} = (x^{p^m})^{-1} = x^{-p^m} = (x^{-1})^{p^m}$, so $x^{-1} \in L$. Thus L is in fact a subfield of K.

Since $m \mid n$, we know that

$$X^{p^n} - X = g(X)(X^{p^m} - X)$$

for some polynomial g. Now the left-hand side has p^n roots in K (every element in K is a root). Then from Lemma 4.3.4 we have

$$K = V(X^{p^n} - X) = V(g) \cup V(X^{p^m} - X).$$

Also we have $|V(g)| \leq \deg(g)$ and $|V(X^{p^m} - X)| \leq p^m$ by Theorem 4.3.5. But then

$$\begin{aligned} p^n &\leq |V(g)| + |V(X^{p^m} - X)| \\ &\leq \deg(g) + p^m \\ &= p^n, \end{aligned}$$

from which we may conclude that $|V(X^{p^m} - X)| = p^m$. Thus the polynomial $X^{p^m} - X$ has p^m roots in K, so $|L| = p^m$.

Ex. 4.39 From the formula given on page 167, there are

$$\begin{aligned} N_3 &= \tfrac{1}{3} \sum_{d \mid 3} \mu(3/d) 11^d \\ &= \tfrac{1}{3}(\mu(3) \cdot 11 + \mu(1) \cdot 11^3) \\ &= \tfrac{1}{3}((-1) \cdot 11 + 1 \cdot 11^3) \\ &= 440 \end{aligned}$$

irreducible monic polynomials of degree 3 in $\mathbb{F}_{11}[X]$.

Ex. 4.40 As above, the explicit formula gives that there are

$$\begin{aligned} N_6 &= \tfrac{1}{6}\sum_{d|6}\mu(6/d)13^d \\ &= \tfrac{1}{6}(\mu(6)\cdot 13+\mu(3)\cdot 13^2+\mu(2)\cdot 13^3+\mu(1)\cdot 13^6) \\ &= \tfrac{1}{6}(1\cdot 13+(-1)\cdot 13^2+(-1)\cdot 13^3+1\cdot 13^6) \\ &= 804076 \end{aligned}$$

irreducible monic polynomials of degree 6 in $\mathbb{F}_{13}[X]$.

If you have access to *Mathematica*, the function `Nirr` defined by

```
Nirr[n_Integer, p_Integer] :=
   (Plus@@(MoebiusMu[n/#]p^#&@Divisors[n]))/n
```

or equivalently

```
Nirr[n_integer, p_Integer] :=
   Apply[Plus[Map[MoebiusMu[n/#]p^#&,
   Divisors[n]]]]/n
```

can be used to easily calculate the number of irreducible monic polynomials of degree n in $\mathbb{F}_p[X]$[5].

Ex. 4.41 Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree d. Then it follows immediately from Theorem 4.8.8 that f divides $X^{p^d}-X$, since f is an irreducible polynomial of degree d, and $d \mid d$.

Similarly, if $c<d$, d does not divide c, and f does not appear among the $f_1,\dots,f_r$, where $f_1\cdots f_r = X^{p^c}-X$ (cf. Theorem 4.8.8). Furthermore, since f is irreducible, f cannot be written as a product of irreducible polynomials; ie. f is not the product of any subset of $\{f_1,\dots,f_r\}$, thus f does not divide $X^{p^c}-X$.

Let $g = X^5+X^4+X^3+2X+2 \in \mathbb{F}_3[X]$. Then $g_1 = \gcd(g, X^3-X) = 1$, $g_2 = \gcd(g, X^9-X) = X^2+X+2$, and $g_3 = \gcd(g, X^{27}-X) = X^3+2X+1$, which may be seen by the Euclidean algorithm. It is easily verified that g_2 and g_3 are irreducible (they have no roots), so the irreducible factorization of g is

$$g = g_2g_3 = (X^2+X+2)(X^3+2X+1)$$

[5] A short explanation of what is going on: Since summation over the divisors of an integer is not directly supported, another approach is necessary. This function first generates a list of the divisors of n (this is the `Divisors[n]`-part). Then the function `MoebiusMu[n/#]p^#` is applied to each element in the list (`#` stands for the independent variable), giving a new list. Finally the elements of the list are added using `Plus@@`, and the result is divided by n.

Ex. 4.42 Let $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Let $R = \mathbb{F}_2[X]/\langle f \rangle$, and consider R as a vector space over $\mathbb{F}_2$ with basis $1, \alpha, \dots, \alpha^5$, where $\alpha = [X] \in R$. Define $F\colon R \to R$ by $F(v) = v^2$; this is a linear map, and the columns of the associated matrix with respect to the chosen matrix may be computed by

$$\begin{aligned}
F(1) &= 1\\
F(\alpha) &= \alpha^2\\
F(\alpha^2) &= \alpha^4\\
F(\alpha^3) &= \alpha^6 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1\\
F(\alpha^4) &= \alpha^8 = \alpha^2\alpha^6\\
&= \alpha^2(\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)\\
&= \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2\\
&= \alpha^7 + \alpha + 1\\
&= \alpha\alpha^6 + \alpha + 1\\
&= \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1\\
&= \alpha\\
F(\alpha^5) &= \alpha^{10} = \alpha^2\alpha^8\\
&= \alpha^3
\end{aligned}$$

ie. the matrix is

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 0\\
0 & 1 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 1\\
0 & 0 & 1 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}$$

One may easily see that this matrix is invertible (adding the last row vector to each of the other rows gives a matrix with exactly one 1 in each row and column, so the determinant is clearly 1), so $\operatorname{Ker} F = \{0\}$.

The matrix for the linear map $F - I$ is

$$\begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0\\
0 & 1 & 0 & 1 & 1 & 0\\
0 & 1 & 1 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 1 & 1 & 1 & 0\\
0 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}$$

Since

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

the polynomial $g = 1 + X + X^2 + X^4 \in \operatorname{Ker}(F - I)$; thus $\mathbb{F}_p \subsetneq \operatorname{Ker}(F - I)$, and f is not irreducible. Further, g satisfies $f \mid g^2 - g$. Then one may use the Euclidean algorithm to find

$$\begin{aligned} \gcd(f, g) &= \gcd(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, X^4 + X^2 + X + 1) \\ &= X^3 + X^2 + 1 \end{aligned}$$

which is a non-trivial factor of f. It may easily be shown that it is irreducible (since it is a polynomial of degree 3 it is sufficient to check that it has no roots in $\mathbb{F}_2$), and dividing f by this factor one gets $X^3 + X + 1$, which is another irreducible factor of f. This is the same result that was obtained in Exercise 32.

Ex. 4.43 Let p be a prime, and let n be such that $p \nmid n$. Let π be an irreducible polynomial of degree d dividing $\Phi_n \in \mathbb{F}_p[X]$. Let $m = \operatorname{ord}([p])$ in the group $(\mathbb{Z}/n\mathbb{Z})^*$ ($[p]$ is a unit, since $\gcd(p, n) = 1$). Let

$$\alpha = [X] \in L = \mathbb{F}_p[X]/\langle \pi \rangle.$$

(i) Since π is irreducible, $\langle \pi \rangle$ is a maximal ideal and L is a field (Proposition 4.6.3). The number of elements in L is p^d by Proposition 4.6.7. Since $\pi \mid \Phi_n$, $[\Phi_n] = 0$ in L. Furthermore, $[\Phi_n] = \Phi_n(\alpha)$; so if we for a moment considers Φ_n as a polynomial in $L[X]$, α is a root of Φ_n. Since $\Phi_n \mid X^n - 1$ α is a root in $X^n - 1$; ie. α is an n'th root. It is not a multiple root, since $(X^n - 1)' = nX^{n-1}$ has no roots besides 0 (since $[n] \neq [0]$ in $\mathbb{F}_p$); in particular α is not a root in nX^{n-1}. Thus by Lemma 4.5.2, α is a primitive n'th root of unity. The number of elements in L^* is $p^d - 1$, and the order of α in L^* is n. Then n divides $p^d - 1$; ie. $p^d \equiv 1 \pmod{n}$.

(ii) Let $L' = \{\xi \in L \mid \xi^{p^m} = \xi\}$. Since $\operatorname{char} L = p$, it follows from Freshman's Dream that $(\xi_1 + \xi_2)^{p^m} = \xi_1^{p^m} + \xi_2^{p^m} = \xi_1 + \xi_2$ when $\xi_1, \xi_2 \in L'$, so $\xi_1 + \xi_2 \in L'$. If $\xi_1^{p^m} = \xi$, then $(-\xi)^{p^m} = -\xi$; since if p is odd, p^m is odd. If $p = 2$ every element is its own additive inverse, so in particular $(-\xi)^{2^m} = \xi^{2^m} = \xi = -\xi$; ie. $-\xi \in L'$. Clearly $(\xi_1\xi_2)^{p^m} = \xi_1^{p^m}\xi_2^{p^m} = \xi_1\xi_2$, so $\xi_1\xi_2 \in L'$. If $\xi \in L' \setminus \{0\}$, then $(\xi^{-1})^{p^m} = (\xi^{p^m})^{-1} = \xi^{-1}$, so $\xi^{-1} \in L'$. Finally, it is clear that $0, 1 \in L'$. This proofs that L' is in fact a subfield of L.

Since $p^m \equiv 1 \pmod{n}$ (by definition of m), we may write $p^m = kn + 1$, and therefore $\alpha^{p^m} = \alpha^{kn+1} = \alpha^{kn}\alpha = \alpha$, since $\alpha^n = 1$. This means $\alpha \in L'$; but then $1, \alpha, \alpha^2, \dots, \alpha^{d-1} \in L'$. This is a basis for L (considered as an $\mathbb{F}_p$ vector space), so we must in fact have $L' = L$. Let β be a generator for L^* (L is a finite field, so the group of units is cyclic). Then β is a primitive $p^d - 1$ root of unity; and since $\beta \in L'$ we have $\beta^{p^m-1} = 1$. Hence $p^d - 1 \mid p^m - 1$, so $d \mid m$, implying $p^d \leq p^m$.

(iii) Since $m = \operatorname{ord}([p])$ in $(\mathbb{Z}/n\mathbb{Z})^*$ and $p^d \equiv 1 \pmod{n}$, we have $[p]^d = 1$, so $m \mid d$. Thus we may conclude that in fact $m = d$. Since the irreducible polynomial π was chosen to be *some* irreducible polynomial dividing Φ_n, this actually shows that *any* irreducible polynomial dividing Φ_n in $\mathbb{F}_p[X]$ has degree m. This means we may write

$$\Phi_n = \pi_1\pi_2\cdots\pi_r, \tag{4.5}$$

where all of the π_i are irreducible polynomials of degree m in $\mathbb{F}_p[X]$. It remains to show that they are distinct.

Consider the equality $X^n - 1 = \prod_{d|n} \Phi_d$. Assume $f \in \mathbb{F}_p[X]$ is some (non-constant and monic) polynomial so that f^2 divides $X^n - 1$. Then by Lemma 4.3.8 $f \mid D(X^n - 1) = nX^{n-1}$. Since p is assumed to not divide n, nX^{n-1} is not the zero polynomial. Since 0 is not a root of $X^n - 1$, it is not a root of f. But the only monic polynomials dividing nX^{n-1} are X^i for $i = 1, \dots, n-1$ (since $\mathbb{F}_p[X]$ is a UFD); this is a contradiction, so no such f can exist. Then certainly, among the π_i, there are no polynomials whose square divides Φ_n; because Φ_n divides $X^n - 1$.

(iv) If Φ_n is irreducible in $\mathbb{F}_p[X]$, there is exactly one polynomial on the right-hand side of the "factorization" (4.5). Since $\deg(\Phi_n) = \varphi(n)$, this is also the degree d of π; which again is the same as the order m of $[p]$ in $(\mathbb{Z}/n\mathbb{Z})^*$. The latter group has exactly $\varphi(n)$ elements, so $[p]$ generates $(\mathbb{Z}/n\mathbb{Z})^*$.

Assume $[p]$ generates $(\mathbb{Z}/n\mathbb{Z})^*$. Then $m = \operatorname{ord}([p]) = \varphi(n)$; this means the degree of each of the π_i is $\varphi(n)$, but still $\deg(\Phi_n) = \varphi(n)$, so there is only one π_i; thus Φ_n is irreducible in $\mathbb{F}_p[X]$.

Ex. 4.44 Since $\mathbb{Q}[X]$ is a Euclidean domain, it is a PID. Thus the ideal $\langle f, g\rangle \subseteq \mathbb{Q}[X]$ is a principal ideal; say generated by h. Now $h \mid f$ in $\mathbb{Q}[X]$, so $f = hr$. But since f is irreducible, one of h and p is a unit; that is, either h or r is a constant (non-zero) polynomial. But we also know that h is a $\mathbb{Q}[X]$-linear combination of f and g, so $h(z) = 0$ meaning that h is not constant. But then $f = r^{-1}h$ divides g because h divides g.

Ex. 4.45 Let $n \geq 1$ and f be an irreducible polynomial dividing Φ_n in $\mathbb{Q}[X]$.

(i) Consider $f \in \mathbb{C}[X]$. Since $\deg f \geq 1$ f has a root ζ in $\mathbb{C}$. But since all roots of f are also roots of Φ_n, this means that ζ is a primitive n'th root of unity.

(ii) Let ζ be some primitive n'th root of unity, and p a prime not dividing n. Assume $f(\zeta) = 0 \Rightarrow f(\zeta^p) = 0$. Let ζ_0 denote the primitive n'th root from (i). Now since ζ_0 is a primitive n'th root, it generates the (multiplicative) group of all n'th roots of unity. In particular, if ζ' is a primitive n'th root, we may write $\zeta' = \zeta_0^k$ for some k. Clearly $\gcd(k, n) = 1$. If $k = p_1 \cdots p_r$, we may define a sequence of primitive n'th roots of unity by $\zeta_1 = \zeta_0^{p_1}, \zeta_2 = \zeta_1^{p_2}, \ldots, \zeta' = \zeta_{r-1}^{p_r}$ (they are all primitive n'th roots because none of the p_i divides n). Using the assumption for f successively we see that $f(\zeta') = 0$; thus every primitive n'th root is a root in f.

(iii) Let $f, g \in \mathbb{Q}[X]$ be monic polynomials. Assume $fg \in \mathbb{Z}[X]$. Let K denote the least common multiple of the denominators of the coefficients of f, and let L denote the least common multiple of the denominators of the coefficients of g (where it is of course assumed that all coefficients are written as reduced fractions with positive denominators). Let $P = Kf$ and $Q = Lg$; write $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ and $Q = b_mX^m + \cdots + b_1X + b_0$. Clearly $a_n = K$ and $b_m = L$. Since K (respectively L) was "the least common multiple", no prime divides all of the a_i (respectively b_i). The goal is to show that $f, g \in \mathbb{Z}[X]$, which amounts to showing that $K = L = 1$. Let p be a prime dividing KL. Then

$$PQ = KLfg = 0 \in \mathbb{F}_p[X]$$

(since P and Q are polynomials with integer coefficients we may reduce the coefficients modulo p). Since p does not divide all of the a_i, there is a largest a_i such that $a_i \not\equiv 0 \pmod{p}$; similarly there is a largest j such that $b_j \not\equiv 0 \pmod{p}$. Then $PQ = a_ib_jX^{i+j}+$terms of lower order. But since $\mathbb{F}_p$ is a domain, $a_ib_j \neq 0$ in $\mathbb{F}_p$; so $PQ \neq 0 \in \mathbb{F}_p[X]$, which is a contradiction. Thus no prime p divides KL; ie. $KL = 1$, so that all denominators in the coefficients of f and g are 1.

(iv) Since $\zeta \in \mathbb{C}$ is a common root of f and $X^n - 1$, by Exercise 44 we have $f \mid X^n - 1$ in $\mathbb{Q}[X]$. Then $\mathbb{Z}[X] \ni X^n - 1 = f(X)g(X)$ where $f, g \in \mathbb{Q}[X]$. Since f is monic, so is g, and thus by (iii) we have $f, g \in \mathbb{Z}[X]$.

(v) Let ζ be a primitive n'th root of unity such that $f(\zeta) = 0$. Let p be a prime number not dividing n, and suppose that $f(\zeta^p) \neq 0$. Since ζ^p is a root in $X^n - 1$ it must be a root in either f or g (cf. the above factorization of $X^n - 1$); thus $g(\zeta^p) = 0$, so ζ is a root in $g(X^p)$. Since f is irreducible and ζ is a common root of $f(X)$ and $g(X^p)$, by Exercise 44 we have $f(X) \mid g(X^p)$.

Write $g(X^p) = f(X)h(X)$ for suitable $h \in \mathbb{Q}[X]$. Then since $g(X) \in \mathbb{Z}[X]$, also $g(X^p) \in \mathbb{Z}[X]$; ie. by (iii) we may conclude that $h(X) \in \mathbb{Z}[X]$ as well. Now we may write $\bar{g}(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in \mathbb{F}_p[X]$, and by Freshman's Dream and the congruence $a^p \equiv a \pmod{p}$

$$\begin{aligned}(\bar{g}(X))^p &= X^{mp} + a_{m-1}^p X^{(m-1)p} + \cdots + a_1^p X^p + a_0^p \\ &= X^{mp} + a_{m-1}X^{(m-1)p} \ldots a_1X^p + a_0 \\ &= \bar{g}(X^p) \in \mathbb{F}_p[X].\end{aligned}$$

If $\pi \in \mathbb{F}_p[X]$ is an irreducible polynomial dividing $\bar{f}$, π divides $\bar{g}(X^p) = (\bar{g}(X))^p$. By irreducibility π divides $\bar{g}$.

(vi) If $\pi \in \mathbb{F}_p[X]$ is some irreducible polynomial dividing both $\bar{f}$ and $\bar{g}$ then π^2 divides $X^n - 1$ (since the equality $X^n - 1 = f(X)g(X)$ also holds after reducing the coefficients modulo p). Then by Lemma 4.3.8 π divides nX^{n-1} which is not the zero polynomial, since $p \nmid n$; since π is irreducible this means $\pi = X$, but X (and hence X^2) does not divide $X^n - 1$. The existence of such a π is therefore impossible.

(vii) Let p be a prime not dividing n, and ζ a primitive n'th root of unity, such that $f(\zeta) = 0$. Assume $f(\zeta^p) \neq 0$.

Then ζ is a root in $g(X^p)$ where g is defined in (iv). From (v), since f and g have integer coefficients, we may consider the corresponding polynomials $\bar{f}$ and $\bar{g}$ in $\mathbb{F}_p[X]$. Since f is monic, $\bar{f} \neq 0$, so $\bar{f}$ has an irreducible factorization in $\mathbb{F}_p[X]$. Let π be one of the irreducible factors of $\bar{f}$; then π divides $\bar{g}$, but this is impossible by (vi). This is a contradiction, so we may conclude that $f(\zeta^p) = 0$. Since f has at least one root by (i), we may from (ii) conclude that every primitive n'th root of unity is a root in f. Since Φ_n is the "least" (lowest degree) polynomial with this property, since f divides Φ_n, and since f is monic, we may conclude that $f = \Phi_n$. f was chosen to be irreducible, so Φ_n is in fact irreducible in $\mathbb{Q}[X]$.

Chapter 5

Ex. 5.1 Let $f, g, h \in R[\mathbb{N}^n]$.

(i) If $f(v) \neq 0$ and $g(v) \neq 0$ for only finitely many $v \in \mathbb{N}^n$, then clearly also $f(v) + g(v) = (f+g)(v)$ is non-zero for finitely many $v \in \mathbb{N}^n$, so $f + g \in R[\mathbb{N}^n]$. Similarly, only finitely many vectors v can be written as a sum of vectors v_1, v_2 for which f, respectively g, is non-zero, so only a finite number of terms occur in the sum

$$(fg)(v) = \sum_{v_1+v_2=v} f(v_1)g(v_2)$$

(defining the empty sum to be $0 \in R$); thus the multiplication is well-defined, and fg is non-zero for only finitely many v, so $fg \in R[\mathbb{N}^n]$.

(ii) From the definition,

$$\begin{aligned}(fg)(v) &= \sum_{v_1+v_2=v} f(v_1)g(v_2)\\ &= \sum_{v_2+v_1=v} g(v_2)f(v_1)\\ &= (gf)(v)\end{aligned}$$

and since this is true for all $v \in \mathbb{N}^n$, $fg = gf$.

(iii) Again, using the definitions,

$$\begin{aligned}(f(g+h))(v) &= \sum_{v_1+v_2=v} f(v_1)(g+h)(v_2)\\ &= \sum_{v_1+v_2=v} f(v_1)(g(v_2)+h(v_2))\\ &= \sum_{v_1+v_2=v} f(v_1)g(v_2) + f(v_1)h(v_2)\\ &= \sum_{v_1+v_2=v} f(v_1)g(v_2) + \sum_{v_1+v_2=v} f(v_1)h(v_2)\\ &= (fg)(v) + (fh)(v)\end{aligned}$$

so $f(g+h) = fg + fh$.

(iv) Finally we have

$$\begin{aligned}(f(gh))(v) &= \sum_{v_1+v_2=v} f(v_1)(gh)(v_2)\\ &= \sum_{v_1+v_2=v} f(v_1) \sum_{w_1+w_2=v_2} g(w_1)h(w_2)\\ &= \sum_{\substack{v_1+v_2=v\\ w_1+w_2=v_2}} f(v_1)g(w_1)h(w_2)\\ &= \sum_{v_1+w_1+w_2=v} f(v_1)g(w_1)h(w_2)\\ &= \sum_{\substack{u+w_2=v\\ v_1+w_1=u}} f(v_1)g(w_1)h(w_2)\\ &= \sum_{u+w_2=v} \left(\sum_{v_1+w_1=u} f(v_1)g(w_1) \right) h(w_2)\\ &= \sum_{u+w_2=v} (fg)(u)h(w_2)\\ &= ((fg)h)(v)\end{aligned}$$

so $f(gh) = (fg)h$.

Ex. 5.2 Let $I = \langle X, Y\rangle \subseteq \mathbb{Q}[X, Y]$. Assume $I = \langle f\rangle$. Now since $Y \in \langle f\rangle$ we have $Y = gf$ for some $g \in \mathbb{Q}[X, Y]$, which means $0 = \deg_X g + \deg_X f$, where $\deg_X(\cdot)$ is the highest power of X, so that $\deg_X f = 0$; that is, f contains no term involving X. Similarly $\deg_Y f = 0$, so that f does not contain terms with Y. This means f is a constant; since $\langle X, Y\rangle$ does not contain any constant polynomials, $\langle f\rangle \neq \langle X, Y\rangle$.

Ex. 5.3 The usual orders $\leq$ on $\mathbb{Z}$ and $\mathbb{R}$ are total orders, but not well orders.

Ex. 5.4 If $\leq$ is a well order on a set S, and $x, y \in S$, consider the subset $M = \{x, y\}$ of S. Since $\leq$ is a well order, this set contains a first element, which means that either $x \leq y$ or $y \leq x$. Thus $\leq$ is a total order.

Ex. 5.5 Let $\leq$ be a term order on $\mathbb{N}^n$, and assume $a \leq b$, $c \leq d$. Then by (iii) in Definition 5.1.2 we have that $a + c \leq b + c$. Also, $c + b \leq d + b$, and since $\leq$ is transitive, we see that $a + c \leq d + b$.

Ex. 5.6 Suppose $v \in \mathbb{R}^2$, and define R_v on $\mathbb{N}^2$ by

$$v_1 R_v v_2 \iff v \cdot v_1 \leq v \cdot v_2$$

where $\cdot$ denotes the usual inner product on $\mathbb{R}^2$ and $\leq$ refers to the usual ordering of $\mathbb{R}$.

(i) $R_{(1,1)}$ is not a partial order, because for instance $(1,1)\cdot(2,1) = 3 = (1,1)\cdot(1,2)$; so $(2,1) \leq (1,2)$ and $(1,2) \leq (2,1)$, but since $(1,2) \neq (2,1)$, $R_{(1,1)}$ is not antisymmetric.

(ii) Clearly $R_{(1,\sqrt{2})}$ is reflexive and transitive (this follows immediately from the corresponding properties for $\leq$ on $\mathbb{R}$). Now assume $(1,\sqrt{2})\cdot v_1 \leq (1,\sqrt{2})\cdot v_2$ and that $(1,\sqrt{2})\cdot v_1 \geq (1,\sqrt{2})\cdot v_2$; ie. $(1,\sqrt{2})\cdot v_1 = (1,\sqrt{2})\cdot v_2$. Writing $v_1 = (a,b)$ and $v_2 = (c,d)$ this means

$$a + b\sqrt{2} = c + d\sqrt{2}$$

but rearranging we see that

$$a - c = (d-b)\sqrt{2}.$$

Since $\sqrt{2}$ is irrational, and a,b,c,d are integers, we must have $d-b=0$, but then also $a-c=0$, so $v_1 = v_2$. Thus $R_{(1,\sqrt{2})}$ is a partial order. It is also a total order, because $\leq$ on $\mathbb{R}$ is. Finally $0 = (1,\sqrt{2})\cdot(0,0) \leq (1,\sqrt{2})\cdot v = a + b\sqrt{2}$ for every $v = (a,b) \in \mathbb{N}^2$, and since $\cdot$ is linear, it is clear that $R_{(1,\sqrt{2})}$ is in fact a term order on $\mathbb{N}^2$.

(iii) As in (ii), one may verify that $R_{(-1,\sqrt{2})}$ is a total order, but it is not a term order, since $(1,0)R_{(-1,\sqrt{2})}(0,0)$.

Ex. 5.7 (i) It is clear from the definition of $\leq_{\text{lex}}$ that it is reflexive ($v = w \Leftrightarrow v_1 = w_1, \ldots, v_n = w_n$) and antisymmetric (because if $v \leq_{\text{lex}} w$ and $v \geq_{\text{lex}} w$, then none of the coordinates may differ). Transitivity may be seen as follows: Assume $v \leq_{\text{lex}} w$ and $w \leq_{\text{lex}} u$, and that $v \neq w$, $w \neq u$ (otherwise it is trivial). Then for some least index i we have $v_i < w_i$ and for some least index j we have $w_j < u_j$. Now if $i < j$ we know that $w_i = u_i$, so that $v_i < u_i$, which again implies $v \leq_{\text{lex}} u$. If $i > j$ then $v_j = w_j < u_j$, so again $v \leq_{\text{lex}} u$. Finally, if $i = j$, $v_i < w_i < u_i$, and therefore $v \leq_{\text{lex}} u$.

Clearly $\leq_{\text{lex}}$ is total, since for any two vectors $v, w \in \mathbb{N}^n$, either $v = w$ or they differ in at least one coordinate; if so, there is a first such coordinate i, so that $v_i < w_i$ or $w_i < v_i$. $0 \leq_{\text{lex}} v$ trivially for any $v \in \mathbb{N}^n$. Since the relations $<$ and $=$ on $\mathbb{N}$ respects $+$ one also sees that $v_1 \leq_{\text{lex}} v_2 \Rightarrow v_1 + v \leq_{\text{lex}} v_2 + v$ holds.

(ii) $\leq_{\text{grlex}}$ is clearly reflexive, because $|v| = |v|$ and $\leq_{\text{lex}}$ is reflexive. If both $v \leq_{\text{grlex}} w$ and $w \leq_{\text{grlex}} v$, then we must have $|v| = |w|$; but then we have both $v \leq_{\text{lex}} w$ and $w \leq_{\text{lex}} w$, so that by the above we have $v = w$. Totality is seen by considering the three cases $|v| < |w|$, $|v| > |w|$ and $|v| = |w|$. In the latter case, we know from above that either $v \leq_{\text{lex}} w$ or $w \leq_{\text{lex}} v$. In the former two cases, the definition of the graded lexicographic order immediately yields $v \leq_{\text{grlex}} w$ or $v \geq_{\text{grlex}} w$, respectively.

Since $0 \leq |v|$ for any $v \in \mathbb{N}^n$, and equality applies only if $v = 0$, we see that $0 \leq_{\text{grlex}} v$. Assume $v_1 \leq_{\text{grlex}} v_2$. If $|v_1| < |v_2|$, then since the norm $|\cdot|$ respects addition (in the sense that $|v + w| = |v| + |w|$), we know that also $|v_1 + v| < |v_2 + v|$, so that $v_1 + v \leq_{\text{grlex}} v_2 + v$. If, on the other hand, $|v_1| = |v_2|$, we know that $v_1 \leq_{\text{lex}} v_2$. But then since $|v_1 + v| = |v_2 + v|$ and $v_1 + v \leq_{\text{lex}} v_2 + v$, we have $v_1 + v \leq_{\text{grlex}} v_2 + v$.

Ex. 5.8 Let $v \in \mathbb{R}^n$ be a vector of non-negative real numbers. Let $u_1, u_2, u_3, u \in \mathbb{N}^n$. Clearly $v \cdot u = v \cdot u$ and $u \leq_{\text{lex}} u$, so that $u \leq_v u$. If $u_1 \leq_v u_2$ and $u_2 \leq_v u_1$, then $v \cdot u_1 \gtrless v \cdot u_2$ is impossible[6], so $v \cdot u_1 = v \cdot u_2$. But this means that both $u_1 \leq_{\text{lex}} u_2$ and $u_2 \leq_{\text{lex}} u_1$ applies, so we must have $u_1 = u_2$. If $u_1 \leq_v u_2$ and $u_2 \leq_v u_3$, there are four cases to consider; three of which are trivial: If $v \cdot u_1 < v \cdot u_2$ or $v \cdot u_2 < v \cdot u_3$, we may conclude that $v \cdot u_1 < v \cdot u_3$, so that $u_1 \leq_v u_3$. The remaining case is $v \cdot u_1 = v \cdot u_2 = v \cdot u_3$, in which case we know that $u_1 \leq_{\text{lex}} u_2$ and $u_2 \leq_{\text{lex}} u_3$, so that $u_1 \leq_{\text{lex}} u_3$; hence $u_1 \leq_v u_3$. This shows that $\leq_v$ is a partial order. It is total because exactly one of the three cases $v \cdot u_1 \gtrless v \cdot u_2$ and $v \cdot u_1 = v \cdot u_2$ applies; in the latter case either $u_1 \leq_{\text{lex}} u_2$ or $u_2 \leq_{\text{lex}} u_1$.

Since v is a vector of non-negative real numbers, $v \cdot u \geq 0$. But this means that $v \cdot 0 = 0 \leq v \cdot u$ for any vector u. Thus if strict inequality applies, $0 \leq_v u$, and if equality applies, we know that $0 \leq_{\text{lex}} u$, so in either case $0 \leq_v u$. The inner product $\cdot$ on $\mathbb{R}^n$ respects addition. This means that if $v \cdot u_1 < v \cdot u_2$, we also have $v \cdot (u_1 + u) < v \cdot (u_2 + u)$, and if $v \cdot u_1 = v \cdot u_2$, we also have $v \cdot (u_1 + u) = v \cdot (u_2 + u)$. In the latter case, we know that $u_1 \leq_{\text{lex}} u_2$ implies $u_1 + u \leq_{\text{lex}} u_2$, so in both cases, $u_1 + u \leq_v u_2 + u$.

Ex. 5.9 Let $\alpha, \beta, \gamma \in \mathbb{N}^n$, and let the relation R on $\mathbb{N}$ be defined by the three (mutually exclusive) cases: $\alpha R \beta \iff$

(I) $\alpha = \beta$

(II) $|\alpha| < |\beta|$

[6] The symbol $\gtrless$ is read "greater than or less than" and is in most cases equivalent to $\neq$.

(III) $|\alpha| = |\beta|$ and the first coordinate pair (α_i, β_i) from the right that is different satisfy $\alpha_i > \beta_i$.

(i) By definition (I), $\alpha R \alpha$, so R is reflexive. Assume $\alpha R \beta$ and $\beta R \alpha$. Then case (II) may be excluded, because if $|\alpha| < |\beta|$ then $\beta R \alpha$ is impossible (and vice versa). We may also exclude case (III), since if $|\alpha| = |\beta|$ and $\alpha_i > \beta_i$, then $\beta R \alpha$ is impossible (and vice versa). Thus we must have $\alpha = \beta$, so R is antisymmetric. If $\alpha R \beta$ and $\beta R \gamma$, there are several cases to consider. If either $|\alpha| < |\beta|$ or $|\beta| < |\gamma|$, we may immediately conclude that $\alpha R \gamma$. If this does not apply, we must have $|\alpha| = |\beta| = |\gamma|$. Now if $\alpha = \beta$ or $\beta = \gamma$ we trivially have $\alpha R \gamma$. The remaining case is that $\alpha_i > \beta_i$ for some index i, and that $\beta_j > \gamma_j$ for some index j. If $i \geq j$ we know that $\alpha_{i+1} = \beta_{i+1} = \gamma_{i+1}, \ldots, \alpha_n = \beta_n = \gamma_n$, that $\alpha_i > \beta_i$ and that $\beta_i \geq \gamma_i$. Thus $\alpha_i > \gamma_i$ and i is the first index (from the right) at which the coordinates of α and γ differ, so $\alpha R \gamma$. The case $j \geq i$ is treated symmetrically. Thus R is transitive.

If $\alpha = \beta$, then $\alpha R \beta$. If $\alpha \neq \beta$, consider the two cases $|\alpha| \gtrless |\beta|$ and $|\alpha| = |\beta|$. In the former case we know that either $\alpha R \beta$ or $\beta R \alpha$. In the latter case, since $\alpha \neq \beta$, there is a largest index i such that α_i and β_i differ; thus for this index i we have $\alpha_i > \beta_i$ or $\alpha_i < \beta_i$, so $\alpha R \beta$ or $\beta R \alpha$. This shows that R is total.

Since $|\alpha| = 0 \Leftrightarrow \alpha = 0$ we see that $0 R \alpha$ (because either $0 = \alpha$ or $|0| = 0 < |\alpha|$). Finally, the cases (I)–(III) are invariant under addition of a vector γ (that is, $\alpha = \beta \Leftrightarrow \alpha + \gamma = \beta + \gamma$, $|\alpha| < |\beta| \Leftrightarrow |\alpha + \gamma| < |\beta + \gamma|$, and if $|\alpha| = |\beta|$, $\alpha \neq \beta$, we also have $|\alpha + \gamma| = |\beta + \gamma|$, and $\alpha_i + \gamma_i > \beta_i + \gamma_i$).

(ii) Let $S \subseteq \mathbb{N}^n$ be a non-empty subset of $\mathbb{N}^n$. Consider the subset $M = |S| = \{|v| \mid v \in S\}$ of $\mathbb{N}$. Since S is non-empty, so is M. This means that M contains a least element, m. Now consider the (non-empty) subset $S' = \{v \in S \mid |v| = m\}$. It is clear that for any vectors $v \in S'$ and $w \in S - S'$ we have vRw (because $m = |v| < |w|$), so a least element of S has to be found in S'. But since S' must be finite (a crude upper limit is $(m+1)^n$ elements), the relation R restricted to S' is a well order on S' (because any total order on a finite set is necessarily a well order). So S' contains a least element v with respect to R; this is also a least element of S with respect to R.

Ex. 5.10 Let $v, w \in \mathbb{N}^2$ and assume that $v \leq_{\text{grlex}} w$. If $v = w$ then clearly also vRw (where R denotes the graded reverse lexicographic order from Exercise 5.9). Assume $v \neq w$. This means that either $|v| < |w|$, in which case vRw, or that

$|v| = v_1 + v_2 = w_1 + w_2 = |w|$ and $v_1 < w_1$. (We cannot have $v_1 = w_1$ because this would imply $v_2 = w_2$ so that $v = w$). But then necessarily $v_2 > w_2$, and we see that vRw.

Assume on the other hand that vRw. Then if $v = w$ or $|v| < |w|$ we have $v \leq_{\text{grlex}} w$. If $|v| = |w|$ and $v \neq w$, then $v_2 > w_2$, so that $v_1 < w_1$, and $v \leq_{\text{grlex}} w$.

Consider the two vectors $(1, 3, 2)$ and $(2, 1, 3)$ in $\mathbb{N}^3$. Then $(1, 3, 2) \leq_{\text{grlex}} (2, 1, 3)$ while $(2, 1, 3)R(1, 3, 2)$, so that the graded lexicographic order and the graded reverse lexicographic order do not coincide in $\mathbb{N}^3$.

Ex. 5.11 Let $\text{in}_\leq(f) = aX^v$ and $\text{in}_\leq(g) = bX^w$. Then $\text{in}_\leq(f)\,\text{in}_\leq(g) = abX^{v+w}$, and since R is a domain, $ab \neq 0$. Let v_i denote any of the vectors such that $f(v_i) \neq 0$ (ie. any vector such that the coefficient of X^{v_i} in f is non-zero). Then by definition of initial term $v \leq v_i$. But then $v + w \geq v_i + w$ since $\geq$ is a term order. Now for fixed i, let w_j denote a vector such that $g(w_j) \neq 0$ (ie. a vector such that the coefficient of X^{w_j} in g is non-zero). Since $w \geq w_j$, we see that $w + v_i \geq w_j + v_i$. By transitivity of $\geq$ we have that $v + w \geq v_i + w_j$. This means that for any way of combining vectors v_i and w_j (that is, for any way of multiplyng terms from f and g), the resulting term is not larger (with respect to $\leq$) than $\text{in}_\leq(f)\,\text{in}_\leq(g)$. Since the latter term has non-zero coefficient, we must have $\text{in}_\leq(fg) = \text{in}_\leq(f)\,\text{in}_\leq(g)$.

Ex. 5.12 We may WLOG assume that $aX^v = \text{in}_\leq(f) = \max(\text{in}_\leq(f), \text{in}_\leq(g))$. If $\text{in}_\leq(g) < \text{in}_\leq(f)$ (where the symbol $<$ of course means $\leq$ and $\neq$), then $g(v) = 0$, so that $(f + g)(v) = a \neq 0$. Clearly $f + g$ cannot contain terms greater than X^v (since such a term would have to appear in f, and aX^v is the initial term of f). Thus in this case we have $\text{in}_\leq(f+g) = \max(\text{in}_\leq(f), \text{in}_\leq(g))$. If $\text{in}_\leq(g) \approx \text{in}_\leq(f)$ (meaning that $\text{in}_\leq(g) = bX^v$), there are two possibilities. Either $a+b \neq 0$, in which case $\text{in}_\leq(f+g) = (a+b)X^v \approx \max(\text{in}_\leq(f), \text{in}_\leq(g))$. Otherwise, every term of $f + g$ is strictly less than X^v; in all cases we see that $\text{in}_\leq(f + g) \leq \max(\text{in}_\leq(f), \text{in}_\leq(g))$.

Ex. 5.13 Let $f = 1+X^5+X+Y+X^3Y+X^4Y+Y^2+2X^2Y^2+XY^3$, and $f_1 = X^3+Y^2$, $f_2 = X^2Y + 1$. Using the lexicographic order $X \geq Y$, we have $\text{in}_\leq(f) = X^3$ and $\text{in}_\leq(g) = X^2Y$. Then[7]

$$f^{(f_1,f_2)} = 1 + X + Y^2 - Y^3$$

(i) $f^{(f_2,f_1)} = 1 - X^2 + Y^2 + XY^3$.

[7] The intermediate calculations have been omitted purposefully. They might appear in a later edition when I learn some more powerful typesetting tricks.

(ii) With $Y \geq X$: $f^{(f_1,f_2)} = 1 - X^3 - X^5 + Y$.

Ex. 5.14 Let $F = (X^2 + Y, X^2Y + 1) \subseteq k[X,Y]$, and let $\leq$ be a term order on $k[X,Y]$. Let $f = Y(X^2 + Y) - (X^2Y + 1) \in I$. Since $\mathrm{in}_{\leq}(X^2Y + 1) = X^2Y$ and $\mathrm{in}_{\leq}(Y^2 - 1) = Y^2$, there are only two cases to consider; $X^2 \geq Y$ and $y \geq X^2$. In the former case, the initial term of f is not divisible by any of the initial terms X^2 and X^2Y. If, on the other hand, $Y \geq X^2$, we may calculate

$$
\begin{array}{lcl}
\underline{Y^2} - 1 & : & (X^2 + \underline{Y}, \underline{X^2Y} + 1) \\
\underline{Y^2 + X^2Y} & & \\
\qquad \underline{-X^2Y} - 1 & & \\
\qquad \underline{-X^2Y - X^2} & & \\
\qquad\qquad\quad \underline{X^2} - 1 & &
\end{array}
$$

Since X^2 is not divisible by any of the initial terms, we see that

$$(Y^2 - 1)^{(X^2+Y, X^2Y+1)} \neq 0$$

regardless of the term order. Thus by Proposition 5.4.2, $(X^2 + Y, X^2Y + 1)$ is not a Gröbner basis with respect to any term order.

Ex. 5.15 Assume $f \in I = \langle f_1, \dots, f_m \rangle \subseteq k[X_1, \dots, X_n]$, and that $F = (f_1, \dots, f_m)$ is a Gröbner basis for I with respect to some term order $\leq$. Let $g \in I$. Since F is a Gröbner basis for I, we know that for some i we have $\mathrm{in}_{\leq}(f_i) \mid \mathrm{in}_{\leq}(g)$; but then the set $(f_1, \dots, f_m, f)$ clearly also constitutes a Gröbner basis for I.

Ex. 5.16 Let $G = (g_1, \dots, g_r)$ and $I = \langle g_1, \dots, g_r \rangle \subseteq k[X_1, \dots, X_n]$. If G is a Gröbner basis then Proposition 5.4.2 immediately gives the desired. Now assume

$$f \in I \Longleftrightarrow f^G = 0$$

for every f in I. We wish to show that G is a Gröbner basis. Let $f \in I$ be any non-zero polynomial. Since $f^G = 0$ (that is, the division algorithm terminates with no remainder), the initial term of f must be divisible by the initial term of one of the g_i; thus G is a Gröbner basis.

Ex. 5.17 Let $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in R$, and consider

$$I = \langle a_1 - b_1, a_2 - b_2, \dots, a_n - b_n \rangle.$$

Let $x_i = a_{i+1} \cdots a_n$ and $y_j = b_1 b_2 \cdots b_{j-1}$. Define $x_n = y_1 = 1 \in R$ (the empty product). Then a little thought shows that

$$x_i y_i b_i = x_{i+1} y_{i+1} a_{i+1}$$

for $i = 1, \dots, n-1$, and using $x_i y_i$ as coefficient we get the telescoping sum

$$\begin{aligned}&x_1y_1(a_1-b_1)+x_2y_2(a_2-b_2)+\cdots+x_ny_n(a_n-b_n)\\&=a_1a_2\cdots a_n-b_1b_2\cdots b_n\end{aligned}$$

which shows that $a_1a_2\cdots a_n - b_1b_2\cdots b_n \in I$.

Now let $I = \langle T_1 - f_1, \dots, T_r - f_r\rangle$. Assume that $f, f_1, \dots, f_r \in k[X_1, \dots, X_n]$ and $f = P(f_1, \dots, f_r)$ for some polynomial $P \in k[T_1, \dots, T_r]$. Then

$$\begin{aligned}f(X_1,\dots,X_n)-P(T_1,\dots,T_r)&=f-P\\&=P(f_1,\dots,f_r)-P(T_1,\dots,T_r).\end{aligned}\tag{5.1}$$

The above shows that any polynomial of the form

$$f_1^{e_1}f_2^{e_2}\cdots f_r^{e_r}-T_1^{e_1}T_2^{e_2}\cdots T_r^{e_r}\tag{5.2}$$

(where the e_i are exponents ≥ 0) belongs to the ideal

$$\langle f_1 - T_1, \dots, f_r - T_r\rangle$$

and hence also to the ideal I. This may be seen by choosing the first e_1 a's and b's to be f_1 and T_1, respectively, and so on. In (5.1), we may collect corresponding terms, and we end up with a sum of polynomials of the form (5.2). Since each of these belong to I, so does

$$f(X_1, \dots, X_n) - P(T_1, \dots, T_r)$$

Ex. 5.18 Let $F = (X^2 + Y, X^2Y + 1) \subseteq \mathbb{Q}[X, Y]$, and let $\leq$ denote the lexicographic order $X \geq Y$. Finally let $f = X^3Y + X^2Y + X + Y^2$.

(i) Since $f = Y(X^2 + Y) + X(X^2Y + 1)$, and since $\operatorname{in}_{\leq}(X^2Y + Y^2) = X^2Y \leq \operatorname{in}_{\leq}(f) = X^3Y$, $\operatorname{in}_{\leq}(X^3Y + X) = X^3Y \leq \operatorname{in}_{\leq}(f) = X^3Y$, by Definition 5.6.2 f reduces to zero modulo F.

(ii) Computation yields

$$\begin{array}{l}\underline{X^3Y}+X^2Y+X+Y^2\quad:\quad(\underline{X^2}+Y,\underline{X^2Y}+1)\\ \underline{X^3Y+XY^2}\\ \qquad\quad\underline{X^2Y}+XY^2+X+Y^2\\ \qquad\quad\underline{X^2Y+Y^2}\\ \qquad\qquad\qquad\underline{XY^2}+X\end{array}$$

and since XY^2 is not divisible by X^2 (and hence neither by X^2Y), $f^F \neq 0$.

Similarly, one gets

$$\begin{array}{lcl}
\underline{X^3Y} + X^2Y + X + Y^2 & : & (\underline{X^2Y} + 1, \underline{X^2} + Y) \\
\underline{X^3Y + X} & & \\
\qquad \underline{X^2Y} + Y^2 & & \\
\qquad \underline{X^2Y + 1} & & \\
\qquad\qquad \underline{Y^2} - 1 & &
\end{array}$$

Y^2 is divisible by neither of the initial terms in F', so also $f^{F'} \neq 0$.

Ex. 5.19 Fix the lexicographic order $X \geq Y$. First we need to find a Gröbner basis for $\langle X^2 + Y, X + Y \rangle$:

$$\mathcal{S}(\underline{X^2} + Y, \underline{X} + Y) = X^2 + Y - X^2 - XY = Y - \underline{XY},$$

which by division with $(X^2 + Y, X + Y)$ gives

$$\begin{array}{lcl}
\underline{-XY} + Y & : & (\underline{X^2} + Y, \underline{X} + Y) \\
\underline{-XY - Y^2} & & \\
\qquad \underline{Y^2} + Y & &
\end{array}$$

Now let $F = (X^2 + Y, X + Y, Y^2 + Y)$. Computing the two relevant $\mathcal{S}$-polynomials gives

$$\begin{aligned}
\mathcal{S}(\underline{X^2} + Y, \underline{Y^2} + Y) &= X^2Y^2 + Y^3 - X^2Y^2 - X^2Y = Y^3 - \underline{X^2Y} \\
\mathcal{S}(\underline{X} + Y, \underline{Y^2} + Y) &= XY^2 + Y^3 - XY^2 - XY = Y^3 - \underline{XY}
\end{aligned}$$

and dividing each of these by F we get

$$\begin{array}{lcl}
\underline{-X^2Y} + Y^3 & : & (\underline{X^2} + Y, \underline{X} + Y, \underline{Y^2} + Y) \\
\underline{-X^2Y - Y^2} & & \\
\qquad \underline{Y^3} + Y^2 & & \\
\qquad \underline{Y^3 + Y^2} & & \\
\qquad\qquad 0 & &
\end{array}$$

and

$$\begin{array}{lcl}
\underline{-XY} + Y^3 & : & (\underline{X^2} + Y, \underline{X} + Y, \underline{Y^2} + Y) \\
\underline{-XY - Y^2} & & \\
\qquad \underline{Y^3} + Y^2 & & \\
\qquad \underline{Y^3 + Y^2} & & \\
\qquad\qquad 0 & &
\end{array}$$

By Remark 5.6.3 and Theorem 5.6.8, this means that F is a Gröbner basis. Since X^2 is divisible by X, we can leave out the generator X^2+Y, ending up with $F' = (\underline{X}+Y, \underline{Y^2}+Y)$. This is easily seen to be a minimal and reduced Gröbner basis; thus it is *the* reduced Gröbner basis by Theorem 5.8.3.

Ex. 5.20 Let $\leq = \leq_{\text{grlex}}$ with $Y \geq X$. Then $F = (\underline{X^2}+Y, X+\underline{Y})$ is in fact a Gröbner basis. This is seen by calculating the $\mathcal{S}$-polynomial

$$\mathcal{S}(\underline{X^2}+Y, X+\underline{Y}) = Y(X^2+Y) - X^2(X+Y) = Y^2 - \underline{X^3}$$

and dividing this by F we get

$$\begin{array}{lcccc}
\underline{-X^3} + Y^2 & : & (\underline{X^2}+Y, X+\underline{Y}) & = & (-X, Y) \\
\underline{-X^3 - XY} & & & & \\
\qquad \underline{Y^2} + XY & & & & \\
\qquad \underline{Y^2 + XY} & & & & \\
\qquad\qquad 0 & & & &
\end{array}$$

so that by Buchberger's $\mathcal{S}$-criterion, F is in fact a Gröbner basis (with respect to the chosen term order).

Ex. 5.21 By Exercise 5.14, $F = (X^2+Y, X^2Y+1)$ is not a Gröbner basis with respect to any term order. Thus in order to decide whether $f = X^3Y + X^3 + X^2Y^3 - X^2Y + XY + X$ lies in the ideal I, one must first calculate a Gröbner basis. Let $\leq$ denote the lexicographic order $X \geq Y$. Then

$$\mathcal{S}(\underline{X^2}+Y, \underline{X^2Y}+1) = Y(X^2+Y) - X^2Y - 1 = \underline{Y^2} - 1,$$

and clearly $(Y^2-1)^F = Y^2-1$. Now let $F' = (X^2+Y, X^2Y+1, Y^2-1)$. Now to ease the calculations a bit, one may observe that $X^2Y+1 = Y(X^2+Y) - (Y^2-1)$, so that F' is a Gröbner basis if and only if $F'' = (X^2+Y, Y^2-1)$ is (this way we only need to calculate one more $\mathcal{S}$-polynomial and do one more polynomial division). Now

$$\mathcal{S}(\underline{X^2}+Y, \underline{Y^2}-1) = Y^2(X^2+Y) - X^2(Y^2-1) = \underline{X^2} + Y^3$$

and

$$\begin{array}{lcccc}
\underline{X^2} + Y^3 & : & (\underline{X^2}+Y, \underline{Y^2}-1) & = & (1, Y) \\
\underline{X^2 + Y} & & & & \\
\quad \underline{Y^3} - Y & & & & \\
\quad \underline{Y^3 - Y} & & & & \\
\qquad 0 & & & &
\end{array}$$

which shows that F'' is a Gröbner basis for $I = \langle X^2 + Y, X^2Y + 1\rangle$. Now Proposition 5.4.2 enables us to decide whether f belongs to I:

$$\begin{array}{lll}
\underline{X^3Y} + X^3 + X^2Y^3 - X^2Y + XY + X & : & (\underline{X^2} + Y, \underline{Y^2} - 1) \\
\underline{X^3Y + XY^2} & & \\
\underline{X^3} + X^2Y^3 - X^2Y - XY^2 + XY + X & & \\
\underline{X^3 + XY} & & \\
\underline{X^2Y^3} - X^2Y - XY^2 + X & & \\
\underline{X^2Y^3 + Y^4} & & \\
\underline{-X^2Y} - XY^2 + X - Y^4 & & \\
\underline{-X^2Y - Y^2} & & \\
\underline{-XY^2} + X - Y^4 + Y^2 & & \\
\underline{-XY^2 + X} & & \\
\underline{-Y^4} + Y^2 & & \\
\underline{-Y^4 + Y^2} & & \\
\qquad\quad 0 & &
\end{array}$$

and the coefficients used during this calculations were $(XY + X + Y^3 - Y, -X - Y^2)$, meaning that

$$\begin{aligned}
&X^3Y + X^3 + X^2Y^3 - X^2Y + XY + X \\
&\qquad\qquad = (XY + X + Y^3 - Y)(X^2 + Y) + (-X - Y^2)(Y^2 - 1).
\end{aligned}$$

Inserting the expression $Y(X^2 + Y) - (X^2Y + 1)$ for $Y^2 - 1$ we obtain

$$\begin{aligned}
&X^3Y + X^3 + X^2Y^3 - X^2Y + XY + X \\
&= (XY + X + Y^3 - Y)(X^2 + Y) \\
&+ (-X - Y^2)(Y(X^2 + Y) - (X^2Y + 1)) \\
&= (X - Y)(X^2 + Y) + (X + Y^2)(X^2Y + 1)
\end{aligned}$$

so we may choose $a_1 = X - Y$ and $a_2 = X + Y^2$.

Ex. 5.22 Let $I = \langle X^2 - Y, Z^3 + Y^2\rangle \subseteq k[X, Y, Z]$ and let $\leq$ denote the lexicographic order given by $X \geq Y \geq Z$.

(i) The initial terms in $(X^2 - Y, Z^3 + Y^2)$ are X^2 and Y^2, respectively. The $\mathcal{S}$-polynomial is

$$\mathcal{S}(\underline{X^2} - Y, Z^3 + \underline{Y^2}) = Y^2(X^2 - Y) - X^2(Z^3 + Y^2) = \underline{-X^2Z^3} - Y^3$$

and since

$$\begin{array}{lcl}
\underline{-X^2Z^3} - Y^3 & : & (\underline{X^2} - Y, Z^3 + \underline{Y^2}) \\
\underline{-X^2Z^3 + YZ^3} & & \\
\qquad\quad \underline{-Y^3} - YZ^3 & & \\
\qquad\quad \underline{-Y^3 - YZ^3} & & \\
\qquad\qquad\qquad 0 & &
\end{array}$$

by Buchberger's $\mathcal{S}$-criterion, $(X^2 - Y, Z^3 + Y^2)$ is a Gröbner basis. It is minimal, because X^2 does not divide Y^2 and vice versa, and the coefficients are both 1. It is reduced because Y is not divisible by Y^2 and Z^3 is not divisible by X^2.

(ii) Polynomial division yields

$$\begin{array}{lcl}
\underline{X^3} - XY + Y^2 + Z^4 + ZY^2 & : & (\underline{X^2} - Y, Z^3 + \underline{Y^2}) \\
\underline{X^3 - XY} & & \\
\qquad\qquad \underline{ZY^2} + Y^2 + Z^4 & & \\
\qquad\qquad \underline{ZY^2 + Z^4} & & \\
\qquad\qquad\qquad\quad \underline{Y^2} & & \\
\qquad\qquad\qquad\quad \underline{Y^2 + Z^3} & & \\
\qquad\qquad\qquad\qquad - Z^3 & &
\end{array}$$

so that by Proposition 5.4.2, $X^3 - XY + Y^2 + Z^4 + ZY^2 \notin I$.

Ex. 5.23 (i) By Exercise 5.20, $(X^2 + Y, X + Y)$ is a Gröbner basis with respect to the graded lexicographic order with $Y \geq X$. Now by Proposition 5.4.2 and the calculation

$$\begin{array}{lcl}
\underline{X^3Y} + X^4 + XY^2 + X^2Y - Y^2 + X^2 & : & (\underline{X^2} + Y, X + \underline{Y}) \\
\underline{X^3Y + XY^2} & & \\
\underline{X^4} + X^2Y - Y^2 + X^2 & & \\
\underline{X^4 + X^2Y} & & \\
\underline{-Y^2} + X^2 & & \\
\underline{-Y^2 - YX} & & \\
\underline{YX} + X^2 & & \\
\underline{YX + X^2} & & \\
0 & &
\end{array}$$

we see that $f = X^3Y + X^4 + XY^2 + X^2Y - Y^2 + X^2 \in I$.

(ii) The coefficients from the above division are $(XY + X^2, -Y + X)$.

Ex. 5.24 Let $I = \langle X^2 + Y^2, X^3 + Y^3\rangle \subseteq \mathbb{Q}[X, Y]$, and let $\leq$ denote the lexicographic order given by $X \geq Y$.

(i) The $\mathcal{S}$-polynomials are

$$\begin{aligned}
S_1 &= \mathcal{S}(\underline{X^2} + Y^2, \underline{X^3} + Y^3) \\
&= X(X^2 + Y^2) - (X^3 + Y^3) \\
&= \underline{XY^2} - Y^3 \\
S_2 &= \mathcal{S}(\underline{X^2} + Y^2, \underline{XY^2} - Y^3) \\
&= Y^2(X^2 + Y^2) - X(XY^2 - Y^3) \\
&= Y^4 + \underline{XY^3}.
\end{aligned}$$

Since S_1 is a $\mathbb{Q}[X, Y]$-linear combination of the generators (X^2+Y^2, X^3+Y^3), clearly $S_1 \in I$. Now by the same reasoning, S_2 is a linear combination of the elements $X^2 + Y^2, S_1 \in I$, so $S_2 \in I$. Combining these results, we see that

$$S_2 - YS_1 = Y^4 + XY^3 - XY^3 + Y^4 = 2Y^4 \in I$$

and finally (since we're looking at $\mathbb{Q}[X, Y]$) we see that $Y^4 \in I$.

(ii) Let $F = (\underline{Y^4}, \underline{XY^2} - Y^3, \underline{X^2} + Y^2)$. In proving that F is a Gröbner basis, the relevant $\mathcal{S}$-polynomials are S_2 and

$$\begin{aligned}
S_3 = \mathcal{S}(\underline{Y^4}, \underline{XY^2} - Y^3) &= XY^4 - Y^2(XY^2 - Y^3) = Y^5 \\
S_4 = \mathcal{S}(\underline{Y^4}, \underline{X^2} + Y^2) &= X^2Y^4 - Y^4(X^2 + Y^2) = -Y^6
\end{aligned}$$

Now clearly $S_3^F = 0$, and $S_4^F = 0$. Thus we only need to check

$$\begin{array}{lcl}
\underline{XY^3} + Y^4 & : & (\underline{Y^4}, \underline{XY^2} - Y^3, \underline{X^2} + Y^2) \\
\underline{XY^3 - Y^4} & & \\
\underline{2Y^4} & & \\
\underline{2Y^4} & & \\
0 & &
\end{array}$$

By Buchberger's $\mathcal{S}$-criterion, F is a Gröbner basis for I with respect to $\leq$. It is minimal because none of the initial terms Y^4, XY^2, and X^2 divide each other and the leading coefficients are all 1. Furthermore it is reduced because Y^2 (and hence also $-Y^3$) is not divisible by any of the initial terms. By uniqueness, F is *the* reduced Gröbner basis for I.

(iii) Let $\leq$ be any term order. By symmetry we may WLOG assume that for this particular term order, $X \geq Y$. Now writing this as $(1,0) \geq (0,1)$, we see that $(2,0) \geq (1,1) \geq (0,2)$, and by the same reasoning $(3,0) \geq (0,3)$. Thus the initial terms of (X^2+Y^2, X^3+Y^3) are X^2 and X^3, respectively. Thus

$$\begin{aligned}\mathcal{S}(\underline{X^2}+Y^2, \underline{X^3}+Y^3) &= X(X^2+Y^2) - (X^3+Y^3)\\ &= XY^2 - Y^3\end{aligned}$$

We cannot tell which term is the initial one with respect to $\leq$, but since this polynomial belongs to I, and since none of the terms is divisible by X^2 (nor X^3), (X^2+Y^2, X^3+Y^3) is not a Gröbner basis.

Ex. 5.25 Let $R = \mathbb{Q}[X,Y,S,T]$ and let $\leq$ denote the lexicographic order given by

$$X \geq Y \geq S \geq T$$

Let $I = \langle S - X^2, T - XY\rangle$.

(i) For simplicity, let $F_1 = (X^2 - S, XY - T)$. Clearly the ideal generated by F_1 is I. Now

$$\mathcal{S}(\underline{X^2} - S, \underline{XY} - T) = Y(X^2 - S) - X(XY - T) = \underline{XT} - YS$$

and since XT is not divisible by any of the initial terms of F_1, we define $F_2 = (X^2 - S, XY - T, XT - YS)$. Now

$$\begin{aligned}\mathcal{S}(\underline{X^2} - S, \underline{XT} - YS) &= T(X^2 - S) - X(XT - YS) = \underline{XYS} - TS\\ \mathcal{S}(\underline{XY} - T, \underline{XT} - YS) &= T(XY - T) - Y(XT - YS) = \underline{Y^2S} - T^2.\end{aligned}$$

Clearly $(XYS - TS)^{F_2} = 0$ (the division requires only one step). The initial term Y^2S of the second $\mathcal{S}$-polynomial is not divisible by any of the initial terms of F_2, so $(Y^2S - T^2)^{F_2} \neq 0$. Hence we define

$$F_3 = (X^2 - S, XY - T, XT - YS, Y^2S - T^2).$$

Once again, we compute some $\mathcal{S}$-polynomials:

$$\begin{aligned}\mathcal{S}(\underline{X^2} - S, \underline{Y^2S} - T^2) &= Y^2S(X^2 - S) - X^2(Y^2S - T^2)\\ &= \underline{X^2T^2} - Y^2S^2\\ \mathcal{S}(\underline{XY} - T, \underline{Y^2S} - T^2) &= YS(XY - T) - X(Y^2S - T^2)\\ &= \underline{XT^2} - YST\\ \mathcal{S}(\underline{XT} - YS, \underline{Y^2S} - T^2) &= Y^2S(XT - YS) - XT(Y^2S - T^2)\\ &= \underline{XT^3} - Y^3S^2\end{aligned}$$

and divide each of these by F_3:

$$\begin{array}{lcl}
\underline{X^2T^2} - Y^2S^2 & : & (\underline{X^2} - S, \underline{XY} - T, \underline{XT} - YS, \underline{Y^2S} - T^2) \\
\underline{X^2T^2 - ST^2} & & \\
\quad\;\; \underline{-Y^2S^2} + ST^2 & & \\
\quad\;\; \underline{-Y^2S^2 + ST^2} & & \\
\qquad\quad 0 & &
\end{array}$$

$$\begin{array}{lcl}
\underline{XT^2} - YST & : & (\underline{X^2} - S, \underline{XY} - T, \underline{XT} - YS, \underline{Y^2S} - T^2) \\
\underline{XT^2 - YST} & & \\
\quad\;\; 0 & &
\end{array}$$

$$\begin{array}{lcl}
\underline{XT^3} - Y^3S^2 & : & (\underline{X^2} - S, \underline{XY} - T, \underline{XT} - YS, \underline{Y^2S} - T^2) \\
\underline{XT^3 - YST^2} & & \\
\quad\;\; \underline{-Y^3S^2} + YST^2 & & \\
\quad\;\; \underline{-Y^3S^2 + YST^2} & & \\
\qquad\quad 0 & &
\end{array}$$

Since all of these divisions leave a remainder of zero, by Buchberger's $\mathcal{S}$-criterion F_3 is a Gröbner basis for I. It is easily seen that none of the initial terms divide each other, and that every leading coefficient is 1, so that F_3 is in fact a minimal Gröbner basis. Furthermore one may by inspection see that F_3 is in fact the reduced Gröbner basis G (since S, T, YS, and T^2 are not divisible by any initial term).

(ii) Since

$$\begin{array}{lcl}
\underline{X^4} + 2X^3Y & : & (\underline{X^2} - S, \underline{XY} - T, \underline{XT} - YS, \underline{Y^2S} - T^2) \\
\underline{X^4 - X^2S} & & \\
\quad\;\; \underline{2X^3Y} + X^2S & & \\
\quad\;\; \underline{2X^3Y - 2XYS} & & \\
\qquad\quad \underline{X^2S} + 2XYS & & \\
\qquad\quad \underline{X^2S - S^2} & & \\
\qquad\qquad\quad \underline{2XYS} + S^2 & & \\
\qquad\qquad\quad \underline{2XYS - 2ST} & & \\
\qquad\qquad\qquad\; S^2 + 2ST & &
\end{array}$$

and none of the terms S^2 and $2ST$ is divisible by any initial term of G, $(X^4+2X^3Y)^G = S^2+2ST \in \mathbb{Q}[S,T]$. Furthermore, substituting X^2 for S and XY for T, we get $Q(X^2,XY) = (X^2)^2 + 2(X^2)(XY) = X^4+2X^3Y$.

(iii) Let $f \in \mathbb{Q}[X,Y]$, $Q = f^G$, and assume $Q \in \mathbb{Q}[S,T]$. Then since

$$\begin{aligned} f(X,Y) &= a\cdot(X^2-S) + b\cdot(XY-T) \\ &\qquad + c\cdot(XT-YS) + d\cdot(Y^2S-T^2) + Q(S,T) \end{aligned}$$

for some $a,b,c,d \in \mathbb{Q}[X,Y,S,T]$, substituting X^2 for S and XY for T shows that

$$\begin{aligned} f(X,Y) &= a\cdot(X^2-X^2) + b\cdot(XY-XY) \\ &\quad + c\cdot(X^2Y-YX^2) + d\cdot(Y^2X^2-(XY)^2) + Q(X^2,XY) \\ &= Q(X^2,XY) \end{aligned}$$

so that $f = f^G(X^2,XY) = Q(X^2,XY)$.

Ex. 5.26 Let $c=(c_1,c_2)\in\mathbb{R}^2$ and let $\cdot$ denote the usual inner product on $\mathbb{R}^2$. Define the relation R_c on $\mathbb{N}^2$ by

$$v_1 R_c v_2 \iff c\cdot v_1 \geq c\cdot v_2$$

(i) R_c is reflexive and transitive because the usual order $\geq$ on $\mathbb{R}$ is reflexive and transitive.

(ii) If $c=(1,0)$ we have $(0,1)R_c(0,2)$ and $(0,2)R_c(0,1)$ (in both cases because $0\geq 0$), but $(0,1)\neq(0,2)$, so that $R_{(1,0)}$ is not antisymmetric.

(iii) Now assume $c_2\neq 0$ and $c_1/c_2\notin\mathbb{Q}$. Assume $v_1R_cv_2$ and $v_2R_cv_1$. Using the definition of R_c and that $\geq$ on $\mathbb{R}$ is antisymmetric, we may conclude that $c\cdot v_1 = c\cdot v_2$, or writing $v_1=(a_1,b_1)$, $v_2=(a_2,b_2)$ we have

$$c_1a_1+c_2b_1 = c_1a_2+c_2b_2$$

which may be rearranged as

$$c_1(a_1-a_2) = c_2(b_2-b_1)$$

If $a_1\neq a_2$ then $c_1/c_2 = (b_2-b_1)/(a_1-a_2)\in\mathbb{Q}$ contrary to the hypothesis. Thus $a_1=a_2$, and since $c_2\neq 0$ this also implies $b_1=b_2$. Thus $v_1=v_2$, and R_c is antisymmetric.

(iv) Let $c = (1, \sqrt{2})$. By (i) and (iii), R_c is a partial order on $\mathbb{N}^2$. It is total because the order $\geq$ on $\mathbb{R}$ is. Clearly $vR_c(0,0)$ for all $v \in \mathbb{N}^2$ (because $a + b\sqrt{2} \geq 0$ for all $(a,b) \in \mathbb{N}^2$). Finally the inner product $\cdot$ is additive, so if $v_1 R_c v_2$ (meaning $c \cdot v_1 \geq c \cdot v_2$) we clearly also have $c \cdot (v_1 + v) \geq c \cdot (v_2 + v)$; i.e. $v_1 + vR_c v_2 + v$. Thus R_c is a term order.

Let $I = \langle X^2 + Y, X^2Y + 1\rangle$. Now $\mathrm{in}_{R_c}(X^2 + Y) = X^2$ because $2 > \sqrt{2}$, and clearly $\mathrm{in}_{R_c}(X^2Y + 1) = X^2Y$. Thus

$$\mathcal{S}(\underline{X^2} + Y, \underline{X^2Y} + 1) = Y(X^2 + Y) - (X^2Y + 1) = \underline{Y^2} - 1.$$

Since Y^2 is not divisible by any of the initial terms, we add $Y^2 - 1$ to our list of generating polynomials, and calculate two new $\mathcal{S}$-polynomials:

$$\begin{aligned} \mathcal{S}(\underline{X^2} + Y, \underline{Y^2} - 1) &= Y^2(X^2 + Y) - X^2(Y^2 - 1) = \underline{Y^3} + X^2 \\ \mathcal{S}(\underline{X^2Y} + 1, \underline{Y^2} - 1) &= Y(X^2Y + 1) - X^2(Y^2 - 1) = \underline{X^2} + Y \end{aligned}$$

Since both of these gives a remainder of zero by division with $F = (\underline{X^2} + Y, \underline{X^2Y} + 1, \underline{Y^2} - 1)$ (the latter is obvious, the former requires two steps), we see by Buchberger's $\mathcal{S}$-criterion that F is in fact a Gröbner basis for I. It is, however, not minimal, since the initial term X^2 divides the initial term X^2Y. Thus $(X^2 + Y, Y^2 - 1)$ is a smaller Gröbner basis for I, and in fact the reduced Gröbner basis with respect to R_c.

(v) Assume $\leq\; = R_c$ for some $c = (c_1, c_2) \in \mathbb{R}^2$. Clearly we must have $c_1, c_2 \geq 0$; otherwise we could find $(v_1, v_2) \in \mathbb{N}$ such that $(0,0)R_c(v_1, v_2)$. Then since $(1,0)R_c(0,n)$ for every $n \in \mathbb{N}$, we see that $c_1 \geq nc_2$ for every $n \in \mathbb{N}$. This implies $c_2 = 0$, but this contradicts R_c being a term order (because $(0,1)R_c(0,2)$ and $(0,2)R_c(0,1)$, while $(0,1) \neq (0,2)$).

Ex. 5.27 Let $\leq$ denote the lexicographic order $Z \geq Y \geq X$ on $\mathbb{Q}[X,Y,Z]$. Then $\mathrm{in}_{\leq}(XZ + Y^2) = XZ$, $\mathrm{in}_{\leq}(X + Y) = Y$, and

$$\mathcal{S}(\underline{XZ} + Y^2, \underline{Y} + X) = Y(XZ + Y^2) - XZ(Y + X) = \underline{-X^2Z} + Y^3$$

which by division with $(XZ + Y^2, X + Y)$ gives

$$\begin{array}{ll} \underline{-X^2Z} + Y^3 & : \quad (\underline{XZ} + Y^2, \underline{Y} + X) = (-X, Y^2) \\ \underline{-X^2Z - XY^2} & \\ \quad \underline{Y^3} + XY^2 & \\ \quad \underline{Y^3 + XY^2} & \\ \qquad 0 & \end{array}$$

Thus $(XZ + Y^2, X + Y)$ is in fact a Gröbner basis with respect to $\leq$. From Proposition 5.4.2 and the calculation

$$\begin{array}{l}
\underline{X^2Z} + Y \quad : \quad (\underline{XZ} + Y^2, \underline{Y} + X) = (X, -XY + X^2 + 1) \\
\underline{X^2Z + XY^2} \\
\qquad \underline{-XY^2} + Y \\
\qquad \underline{-XY^2 - X^2Y} \\
\qquad\qquad \underline{X^2Y} + Y \\
\qquad\qquad \underline{X^2Y + X^3} \\
\qquad\qquad\qquad \underline{Y} - X^3 \\
\qquad\qquad\qquad \underline{Y + X} \\
\qquad\qquad\qquad\qquad - X^3 - X
\end{array}$$

we see that $X^2Z + Y \notin \langle XZ + Y^2, X + Y \rangle$.

Ex. 5.28 Let $I = \langle X^2 + Y, X^2Y + 1 \rangle \subseteq \mathbb{Q}[X, Y]$, and let $\leq$ denote the lexicographic term order $Y \geq X$.

(i) We have $\mathcal{S}(\underline{Y} + X^2, \underline{X^2Y} + 1) = X^2(Y + X^2) - (X^2Y + 1) = \underline{X^4} - 1$. None of the initial terms divide X^4, so we add it to the list, thus obtaining $(Y + X^2, X^2Y + 1, X^4 - 1)$. The next two $\mathcal{S}$-polynomials are

$$\begin{aligned}
\mathcal{S}(\underline{Y} + X^2, \underline{X^4} - 1) &= X^4(Y + X^2) - Y(X^4 - 1) = \underline{Y} + X^6 \\
\mathcal{S}(\underline{X^2Y} + 1, \underline{X^4} - 1) &= X^2(X^2Y + 1) - Y(X^4 - 1) = \underline{Y} + X^2
\end{aligned}$$

The latter clearly leaves a remainder of zero by division with $(Y + X^2, X^2Y + 1, X^4 - 1)$; the former requires a computation:

$$\begin{array}{l}
\underline{Y} + X^6 \quad : \quad (\underline{Y} + X^2, \underline{X^2Y} + 1, \underline{X^4} - 1) = (1, 0, X^2) \\
\underline{Y + X^2} \\
\qquad \underline{X^6} - X^2 \\
\qquad \underline{X^6 - X^2} \\
\qquad\quad 0
\end{array}$$

Thus $(Y + X^2, X^2Y + 1, X^4 - 1)$ is in fact a Gröbner basis for I with respect to $\leq$. Since $X^2Y + 1 = X^2(Y + X^2) - (X^4 - 1)$ we see that we may leave out the middle generator, giving the (reduced) Gröbner basis $(Y + X^2, X^4 - 1)$.

(ii) Clearly $X^4 - 1 \in I$ (by (i)). In Exercise 5.26(iv) another Gröbner basis for I was found; which contained $Y^2 - 1$, so clearly also $Y^2 - 1 \in I$.

(iii) Let $\leq$ be an arbitrary term order and let

$$F = (f_1, f_2, f_3) = (X^2 + Y, Y^2 - 1, X^4 - 1).$$

If $X^2 \geq Y$ we know by Lemma 5.7.3 that $\mathcal{S}(f_1, f_2) \rightarrow_F 0$. Since I may be generated by f_1 and f_2 alone (cf. Exercise 5.26(iv)), (f_1, f_2) is a Gröbner basis for I; thus in this case $F = (f_1, f_2, f_3)$ is certainly also a Gröbner basis. In the case $Y \geq X^2$, we may again use Lemma 5.7.3; this time to conclude that $\mathcal{S}(f_1, f_3) \rightarrow_F= 0$, so also in this case F is a Gröbner basis.

Ex. 5.29 Let

$$I = \langle x^5 + y^3 + z^2 - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1\rangle \in \mathbb{Q}[x, y, z].$$

In order to use Lemma 5.7.3 and Theorem 5.6.8, we must find a term order $\leq$ such that the three initial terms have no common divisor; thus in this case we must find a term order such that the three initial terms are powers of x, y, and z, respectively. Let $v = (a, b, c) \in \mathbb{R}^3$, where a, b, c are positive numbers. We must determine a, b, c such that in the matrix

$$\begin{pmatrix} 5a & 3b & 2c \\ 2a & 2b & c \\ 6a & 5b & 3c \end{pmatrix}$$

there is exactly one row where the first entry is greatest, one row where the second entry is greatest, and one row in which the third element is greatest. The first thing to note is that if we have such a triple (a, b, c), then every triple of the form (ka, kb, kc) where $k > 0$ is also a solution. Thus we may WLOG choose $a = 1$. If the row where the first element is greatest is the second, then $c < 2$, but then $2c < 4 < 5$ and $3c < 6$, so that no row can exist where the third element is greatest. The same argument applies to the last row; if $6a = 6$ is greater than $5b$ and $3c$, then $c < 2 = 2a$ and $2c < 5 = 5a$. Thus we may conclude that the row in which the first element is greatest has to be the first row. Furthermore, we now know that $c < 5/2$ and $b < 5/3$. But if the third element of one of the remaining rows is greatest, then we must also have $c > 2$. Choosing $c = 9/4$ we have the situation

$$\begin{pmatrix} 5 & 3b & 9/2 \\ 2 & 2b & 9/4 \\ 6 & 5b & 27/4 \end{pmatrix}$$

and we see that we must choose $b > 1$. Luckily, $b = 4/3$ works:

$$\begin{pmatrix} 5 & 4 & 9/2 \\ 2 & 8/3 & 9/4 \\ 6 & 20/3 & 27/4 \end{pmatrix} \approx \begin{pmatrix} 5.00 & 4.00 & 4.50 \\ 2.00 & 2.67 & 2.25 \\ 6.00 & 6.67 & 6.75 \end{pmatrix}$$

Multiplying through by 12 we may set $v = (12, 16, 27)$. This gives a term order on $\mathbb{N}^3$ by Exercise 5.8. With respect to this term order, we have

$$\begin{aligned} F &= (f_1, f_2, f_3) \\ &= (\underline{x^5} + y^3 + z^2 - 1, x^2 + \underline{y^2} + z - 1, x^6 + y^5 + \underline{z^3} - 1). \end{aligned}$$

Then by Lemma 5.7.3 we have $\mathcal{S}(f_i, f_j) \to_{(f_i,f_j)} 0$ for $1 \le i < j \le 3$. But then clearly also $\mathcal{S}(f_i, f_j) \to_F 0$ for $1 \le i < j \le 3$, so that by Theorem 5.6.8, F is a Gröbner basis.

Ex. 5.30 Let X be any subset of k^n, where k is a field. Define

$$I(X) = \{f \in k[X_1, \dots, X_n] \mid f(a_1, \dots, a_n) = 0 \forall (a_1, \dots, a_n) \in X\}.$$

That is, $I(X)$ consists of the polynomials $f \in k[X_1, \dots, X_n]$ for which every element of X is a root.

Clearly, if $f_1, f_2 \in I(X)$ then also $f_1 + f_2 \in I(X)$. The zero polynomial has every element of k^n as a root; thus in particular every element of X, so $0 \in I(X)$. If $f(a) = 0$ for every $a = (a_1, \dots, a_n) \in X$ then also $(-f)(a) = -(f(a)) = 0$ for every $a \in X$. Thus $I(X)$ is a group (with respect to $+$). If $f \in I(X)$ and $\lambda \in k[X_1, \dots, X_n]$ is any polynomial, then $(\lambda f)(a) = \lambda(a) f(a) = 0$ for every $a \in X$, so $\lambda f \in I(X)$. Thus $I(X)$ is in fact an ideal.

Let $a \in X$ and $f \in I(X)$ be arbitrary. Then by definition, $f(a) = 0$, so that $a \in V(I(X))$. Since a was arbitrary, this shows $X \subseteq V(I(X))$. ($X = \emptyset$ is a trivial special case).

It is clear that if $X \subseteq Y$, then $I(X) \supseteq I(Y)$. Thus we have in particular $I(X) \supseteq I(V(I(X)))$.

Let $f \in I(X)$. We wish to show $f \in I(V(I(X)))$; that is, we wish to show

$$f(b) = 0 \text{ for every } n\text{-tuple } b = (b_1, \dots, b_n) \in V(I(X)).$$

Let $b \in V(I(X))$. This means that for any $g \in I(X)$ we have $g(b) = 0$. But this is in particular true for $g = f$, thus $f(b) = 0$. Since b was arbitrary, we have $f \in I(V(I(X)))$.

Ex. 5.31 Let $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ and $I = \langle f_1, \dots, f_m \rangle$. Since $\{f_1, \dots, f_m\} \subseteq I$, clearly $V(I) \subseteq V(f_1, \dots, f_m)$.

Now assume $a = (a_1, \dots, a_n) \in k^n$ is a common root of $f_1, \dots, f_m$; that is, $a \in V(f_1, \dots, f_m)$. Let $f \in I$ be arbitrary. We may write $f = \lambda_1 f_1 + \dots + \lambda_m f_m$ for suitable $\lambda_i \in k[X_1, \dots, X_n]$. But then $f(a) = \lambda_1(a) f_1(a) + \dots + \lambda_m(a) f_m(a) = 0 + \dots + 0 = 0$, so that $a \in V(I)$. Thus $V(I) = V(f_1, \dots, f_m)$.

Ex. 5.32 Let

$$I = \langle 5x + y + z - 17, x + y - z - 1, x + y + z - 9 \rangle \subseteq \mathbb{R}[x, y, z]$$

and let $\leq$ denote the lexicographic order $x \geq y \geq z$. By subtracting suitable multiples (5 and 1) of the third generator from the first two, we get

$$\begin{aligned} I &= \langle -4y - 4z + 28, -2z + 8, x + y + z - 9 \rangle \\ &= \langle y + z - 7, z - 4, x + y + z - 9 \rangle \end{aligned}$$

By Lemma 5.7.3 and Theorem 5.6.8, this last expression is a Gröbner basis for I (in fact a minimal one). Further reduction to the reduced Gröbner basis proceeds exactly as if one was doing Gaussian elimination on the system of linear equations (except that we do not insert the solution $z = 4$; rather we subtract the polynomial $z - 4$ from the other generators), thus obtaining

$$\begin{aligned} I &= \langle y - 3, z - 4, x + y - 5 \rangle \\ &= \langle y - 3, z - 4, x - 2 \rangle. \end{aligned}$$

This is easily seen to be the reduced Gröbner basis for I with respect to $\leq$.