A First Course in Abstract Algebra
by Anderson & Feil

Frosty

January 11, 2026

Contents

1 The Natural Numbers

Problem 1

Prove using mathematical induction that for all positive integers n,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Proof. Let $n = 1$ then $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{1(2)}{2} = 1$. Assume the formula is true for some integer $k = n - 1$, thus:

$$1 + 2 + 3 + \cdots + (n-1) = \frac{(n-1)((n-1)+1)}{2}$$

Thus:

$$\begin{aligned}
&1 + 2 + 3 + \cdots + (n-1) + n \\
&= \frac{(n-1)((n-1)+1)}{2} + n \\
&= \frac{(n-1)^2 + n - 1}{2} + \frac{2n}{2} \\
&= \frac{(n-1)^2 + 3n - 1}{2} \\
&= \frac{n^2 - 2n + 1 + 3n - 1}{2} \\
&= \frac{n(n+1)}{2}
\end{aligned}$$

∎

Problem 3

You probably recall from your previous mathematical work the *triangle inequality:* for any real numbers x and y,

$$|x + y| \leq |x| + |y|$$

Accepts this as given (or see a calculus text to recall how it is proved). Generalize the triangle inequality, by proving that

$$|x_1 + x_2 + \cdots + x_n \leq |x_1| + |x_2| + \cdots |x_n|,$$

for any positive integer n.

Proof. For $n = 1$, trivially $|x_1| \leq |x_1|$. For $n = 2$, $|x_1 + x_2| \leq |x_1| + |x_2|$ by the triangle inequality. Now assume the formula holds for $k = n - 1$, thus:

$$|x_1 + x_2 + \cdots + x_{n-1}| \leq |x_1| + |x_2| + \cdots |x_{n-1}|$$

Thus:

$$\begin{aligned}
&|x_1 + x_2 + \cdots + x_{n-1} + x_n| \\
&\leq |(x_1 + x_2 + \cdots + x_{n-1}) + x_n| \\
&\leq |x_1 + x_2 + \cdots + x_{n-1}| + |x_n| && \text{triangle inequality} \\
&\leq |x_1| + |x_2| + \cdots + |x_n|
\end{aligned}$$

∎

Problem 4

Given a positive integer n, recall that $n! = 1 \cdot 2 \cdot 3 \cdots$ (this is read as n factorial). Provide an inductive definition for $n!$. (It is customary to actually start this defintion at $n = 0$, setting $0! = 1$)

Solution

We can define $n!$ as follows. If $n <= 1$, then $n! = 1$. If $n > 1$, then $n! = n(n-1)!$.

Problem 5

Prove that $2^n < n!$ for all $n \geq 4$.

Proof. Let $n = 4$, then $2^4 = 16 < 4! = 24$. Assume the inequality holds for $k = n - 1$, thus:

$$2^{n-1} < (n-1)!$$

Thus:

$$\begin{aligned} &2^{n-1} \cdot 2 < (n-1)! \cdot n \quad \text{Note: } 2 < 4 \leq n \\ &2^n < n! \end{aligned}$$

∎

Problem 7

Prove the familiar geometric progression formula. Namely, suppose that a and r are real numbers with $r \neq 1$. Then show that:

$$a + ar + ar^2 + \cdots + ar^{n-1} = \frac{a - ar^n}{1 - r}$$

Proof. Let $n = 1$, then $a = \frac{a-ar^n}{1-r} = \frac{a-ar}{1-r} = \frac{a(1-r)}{1-r} = a$. Assume the formula holds for $k = n - 1$, thus:

$$a + ar + ar^2 + \cdots + ar^{n-2} = \frac{a - ar^{n-1}}{1 - r}$$

Thus

$$\begin{aligned} &a + ar + ar^2 + \cdots + ar^{n-2} + ar^{n-1} \\ &= \frac{a - ar^{n-1}}{1 - r} + ar^{n-1} \\ &= \frac{a - ar^{n-1}}{1 - r} + \frac{(1-r)ar^{n-1}}{1 - r} \\ &= \frac{a - ar^{n-1} + (1-r)(ar^{n-1})}{1 - r} \\ &= \frac{a - ar^{n-1} + ar^{n-1} - ar^n}{1 - r} \\ &= \frac{a - ar^n}{1 - r} \end{aligned}$$

∎

Problem 12

Consider the sequence a_n defined inductively as follows:

$$a_1 = 5, a_2 = 7, a_{n+2} = 3a_{n+1} - 2a_n$$

Proof. Let $n = 1$, then $a_1 = 5 = 3 + 2^n = 3 + 2^1 = 5$. Let $n = 2$, then $a_2 = 7 = 3 + 2^n = 3 + 2^2 = 7$ Assume the formula holds for $k < n$ thus:

$$a_{n-1} = 3 + 2^{n-1}$$

and

$$a_{n-2} = 3 + 2^{n-2}$$

So $k = n$ is:

$$a_n = 3a_{n-1} - 2a_{n-2} = 3(3 + 2^{n-1}) - 2(3 + 2^{n-2})$$

Then:

$$\begin{aligned}
&3(3 + 2^{n-1}) - 2(3 + 2^{n-2}) \\
&= 9 + 3 \cdot 2^{n-1} - 6 - 2 \cdot 2^{n-2} \\
&= 3 + 3 \cdot 2^{n-1} - 2^{n-1} \\
&= 3 + 2 \cdot 2^{n-1} \\
&= 3 + 2^n
\end{aligned}$$

∎

Problem 14

In this problem you will prove some results about the binomial coefficients, using induction. Recall that:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

where n is a positive integer, and $0 \leq k \leq n$.
(a) Prove that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$n \geq 2$ and $k < n$. Hint: You do not need induction to prove this. Bear in mind that $0! = 1$.
(b) Verify that $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$. Use these facts, together with part a, to prove by induction on n that $\binom{n}{k}$ is an integer, for all k with $0 \leq k \leq n$. (Note: You may have encountered $\binom{n}{k}$ as the count of the number of k element subsets of a set of n objects; it follows that from this $\binom{n}{k}$ is an integer. What we are asking for here is an inductive proof based on algebra.)
(c) Use part a and induction to prove the Binomical Theorem: For non-negative n and variables x, y,

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Proof.

$$
\begin{aligned}
&\binom{n-1}{k} + \binom{n-1}{k-1} \\
&= \frac{(n-1)!}{((n-1)-k)!k!} + \frac{(n-1)!}{((n-1)-(k-1))!(k-1)!} \\
&= (n-1)!\left(\frac{1}{((n-1)-k)!k!} + \frac{1}{((n-1)-(k-1))!(k-1)!}\right) \\
&= (n-1)!\left(\frac{1}{((n-1)-k)!k(k-1)!} + \frac{1}{((n-1)-(k-1))!(k-1)!}\right) \\
&= \frac{(n-1)!}{(k-1)!}\left(\frac{1}{((n-1)-k)!k} + \frac{1}{((n-1)-(k-1))!}\right) \\
&= \frac{(n-1)!}{(k-1)!}\left(\frac{1}{(n-k-1)!k} + \frac{1}{(n-k)!}\right) \\
&= \frac{(n-1)!}{(k-1)!}\left(\frac{1}{(n-k-1)!k} + \frac{1}{(n-k)(n-k-1)!}\right) \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{1}{k} + \frac{1}{(n-k)}\right) \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{n-k}{k(n-k)} + \frac{k}{k(n-k)}\right) \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{n}{k(n-k)}\right) \\
&= \frac{n!}{k!(n-k)!}
\end{aligned}
$$

∎

Proof. Let $k = 0$ then, $\binom{n}{0} = \frac{n!}{(n-0)!(0!)} = \frac{n!}{n!} = 1 \in \mathbb{Z}$. Let $k = n$ then, $\binom{n}{n} = \frac{n!}{(n-n)!(n!)} = \frac{n!}{n!} = 1 \in \mathbb{Z}$. Assume this holds for $n-1$, thus for all k where $0 \leq k \leq n-1$:

$$\binom{n-1}{k} \in \mathbb{Z}$$

Then:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Since each of these terms exist in $\mathbb{Z}$ their sum $\binom{n}{k}$ is in $\mathbb{Z}$ since the integers are closed over addition. ∎

Proof. Let $n = 0$. Then:

$$(x+y)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} = \binom{0}{0} x^0 y^0 = 1 \cdot 1 \cdot 1 = 1$$

Assume the formula holds for $n-1$, thus:

$$\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} = (x+y)^{n-1}$$

Then:

$$\begin{aligned}
(x+y)^n &= (x+y)^{n-1} \cdot (x+y) \\
&= \left(\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} \right) \cdot (x+y) \\
&= x \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} + y \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \left(\binom{n-1}{k-1} + \binom{n-1}{k} \right) x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}
\end{aligned}$$

∎

Problem 15

Criticize the following "proof" showing that all cows are the same color.
It suffices to show that any herd of n cows has the same color. If the herd has but one cow, then trivially all the cows in the herd have the same color. Now suppose that we have a herd of n cows and $n > 1$. Pick out a cow and remove it from the herd, leaving $n - 1$ cows; by the induction hypothesis these cows all have the same color. Now put the cow back and remove another cow. (We can do so because $n > 1$.) The remaining $n - 1$ again must all be the same color. Hence, the first cow selected and the second cow selected have the same color as those not selected, and so the entire herd of n cows has the same color.

Solution

The proof selects a different set of $n - 1$ cows each time.

Problem 16

Prove the converse of Theorem 1.1; that is, prove that the Principle of Mathematical Induction implies the Well-ordering Princple. (This shows that these two principles are logically equivalent, and so from an axiomatic point of view it doesn't matter which we assume is an axiom for the natural numbers.)

Proof. Assume that the principle of mathematical induction holds. Let $G \subseteq \mathbb{N}$ be nonempty. For contradiction, suppose G has no least element. Define $P(n)$ to be the statement: "Nothing $\leq n$ is in G."

If $1 \in G$, then 1 would be the least element of G, a contradiction. So $1 \notin G$ and $P(1)$ is true.

Assume $P(n)$ holds meaning no element of G is $\leq n$. If $n+1 \in G$, then $n+1$ would be the least element of G, a contradiction. Therefore $n+1 \notin G$, and hence $P(n+1)$ holds.

By induction, $P(n)$ holds for all $n \in \mathbb{N}$. So no element of $\mathbb{N}$ is in G, so $G = \emptyset$, contradicting the assumption that G is nonempty. ∎

2 The Integers

Problem 3

Prove that the set of all linear combinations of a and b are precisely the multiple of $\gcd(a, b)$.

Proof. Let a, b be integers such that $a \neq 0$ or $b \neq 0$. We know $ax + by = \gcd(a, b)$ for some $x, y \in \mathbb{Z}$. Let t be an arbitrary integer. Then $t(ax + by) = t(\gcd(a, b))$. It follows that $a(tx) + b(ty) = t(\gcd(a, b))$ Showing that any integer multiple t of the $\gcd(a, b)$ is equivalent to some linear combination of a, b.

Let a, b, x, and y be arbitrary integers. Let $d = \gcd(a, b)$. It follows that $d \mid a$ and $d \mid b$. Then $a = dt$ for some $t \in \mathbb{Z}$ and $b = df$ for some $f \in \mathbb{Z}$. Then:

$$ax + by = dtx + dfy = d(tx + fy)$$

So any linear combination of a and b is a multiple of the $\gcd(a, b)$. ∎

Problem 4

Two numbers are said to be relatively prime if their gcd is 1. Prove a, b relatively prime if and only if every integer can be written as a linear combination of a and b.

Proof. $\rightarrow$ Suppose $a, b \in \mathbb{Z}$ are relatively prime. Let $d \in \mathbb{Z}$. Since a, b are relatively prime $\gcd(a, b) = ax + by = 1$ where $x, y \in \mathbb{Z}$. Then $d(\gcd(a, b)) = d(ax + by) = a(dx) + b(dy) = d(1) = d$.

$\leftarrow$ Suppose every integer can be written as a linear combination of a and b. In particular $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Then $\gcd(a, b) = 1 = ax + by$ so a and b are relatively prime. ∎

Problem 5

Prove Theorem 2.6. That is, use induction to prove that if the prime p divides $a_1 a_2 \cdots a_n$, then p divides a_i for some i.

Proof. Suppose p is prime.

Base case: If $p \mid a_1 a_2$ by definition of being prime $p \mid a_1$ or $p \mid a_2$.

Assume the Theorem holds for $n - 1$ so if $p \mid a_1 a_2 \cdots a_{n-1}$ then $p \mid a_i$ for some i. Now suppose $p \mid a_1 a_2 \cdots a_{n-1} a_n$. Let $c = a_1 a_2 \cdots a_{n-1}$, then $p \mid c \cdot a_n$. By definition of being prime $p \mid c$ by the induction hypothesis or $p \mid a_n$. ∎

Problem 6

Suppose that a and b are positive integers. If $a + b$ is prime, prove that $\gcd(a, b) = 1$.

Proof. We've already proved n is prime iff n is irreducible. Suppose $a + b$ is prime and for contradiction $\gcd(a, b) = x > 1$. Since $a + b$ is prime it has no factors other than itself and 1. Since $\gcd(a, b) = x > 1$ then $x \mid a$ and $x \mid b$. Furthermore, $a = tx$ and $b = yx$ for some $t, y \in \mathbb{Z}$. Then $a + b = tx + yx = x(t + y)$ a contradiction since $a + b$ is prime. ∎

Problem 7

(a) A natural number greater than 1 that is not prime is called composite. Show that for any n, there is a run of n consecutive composite numbers. Hint: Think Factorial.

(b) Therefore, there is a string of 5 consecutive composite numbers starting where?

Proof. Let $T = \{2, 3, \ldots, n+1\}$ and let i be an element in T. Now let

$$d = i + (n+1)!.$$

First notice $2 \leq i \leq n+1$. Then:

$$((i+1) + (n+1)!) - (i + (n+1)!) = 1$$

Showing consecutive values of i produce consecutive values of d. Since $2 \leq i \leq n+1$, we have $i \mid (n+1)!$. Then:

$$\begin{aligned} d &= i + (n+1)! \\ &= i\left(1 + \frac{(n+1)!}{i}\right) \end{aligned}$$

Clearly d is a composite number since it has been factored into 2 integers greater than 1. Thus, the n values of d produce a sequence of n consecutive composite numbers. ∎

Solution (b):

$$722 = 2 \cdot 361, 723 = 3 \cdot 241, 724 = 2 \cdot 362, 725 = 5 \cdot 145, 726 = 2 \cdot 363$$

Problem 9

Notice that $\gcd(30, 50) = 5\gcd(6, 10) = 5 \cdot 2$. In fact, this is always true; prove that if $a > 0$, then $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

Proof. Let $p = \gcd(ab, ac) = abx + acy$. Since $a \mid p$ there exists r such that $p = ar$. So $ar = abx + acy$ and dividing by a gives $r = bx + cy$. Since $a > 0$ and $ar = \gcd(ab, ac) > 0$ it follows that $r > 0$. Thus r is a positive linear combination of b and c. Suppose, for contradiction, there exists d that is a positive linear combination of b and c, and $d < r$. So $d = bu + cv$ for some integers u, v. Since $a > 0$ it follows that $ad > 0$. But then $ad = abu + acv$ and $ad < ar = p$ contrdicting the minimality of p. Therefore $r = \gcd(b, c)$. It follows that $\gcd(ab, ac) = ar = a \cdot \gcd(b, c)$. ∎

Problem 10

Suppose two integers a and b have been factored into primes as follows:

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

and

$$b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the p_i's are primes, and the exponents m_i and n_i are non-negative integers. It is the case that

$$\gcd(a, b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$$

where s_i is the smaller of n_i and m_i. Show this with $a = 360 = 2^3 \cdot 3^2 \cdot 5$ and $b = 2^2 3^2 5^2$. Now prove this fact in general.

Solution:

Let

$$a = 360 = 2^3 \cdot 3^2 \cdot 5^1, \quad b = 2^2 \cdot 3^2 \cdot 5^2.$$

Exponents of each prime factor:

Prime p_i	Exponent in a (n_i)	Exponent in b (m_i)
2	3	2
3	2	2
5	1	2

Minimum exponent for each prime:

$$s_i = \min(n_i, m_i)$$

Prime p_i	$s_i = \min(n_i, m_i)$
2	2
3	2
5	1

Multiply the primes raised to the minimum exponents:

$$\gcd(a, b) = 2^2 \cdot 3^2 \cdot 5^1 = 4 \cdot 9 \cdot 5 = 180.$$

The gcd of 360 and 900 is 180.

Proof. Let $a = \prod_{i=1}^{r} p_i^{n_i}$ and $b = \prod_{i=1}^{r} p_i^{m_i}$. For each prime p_i, define $s_i = \min(n_i, m_i)$ and let $c_i = p_i^{s_i}$.

First note that the gcd will have the common prime factors of a and b. A prime not common to both would not divide both.

Let $f_i = p_i^{s_i+1}$ for the ith prime number appearing in a and b. Then $f_i > p_i^{m_i}$ or $f_i > p_i^{n_i}$ so $f_i \nmid p_i^{m_i}$ or $f_i \nmid p_i^{n_i}$. So c_i is the largest power of p_i dividing the ith prime of both numbers.

Since the primes are independent, the greatest common divisor of a and b is $\gcd(a, b) = \prod_{i=1}^{r} c_i = \prod_{i=1}^{r} p_i^{s_i}$. ∎

Problem 11

The **least common multiple** of natural numbers a and b is the smallest positive common multiple of a and b. That is, if m is the least common mulitple of a and b, then $a \mid m$ and $b \mid m$, and if $a \mid n$ and $b \mid n$ then $n \geq m$. We will write $lcm(a, b)$ for the least common mulitple of a and b. Can you find a formula for the lcm of the type given for the gcd in the previous excersize.

Solution

Suppose two integers a and b have been factored into primes as follows:

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

and

$$b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the p_i's are primes, and the exponents m_i and n_i are non-negative integers. It is the case that

$$lcm(a, b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$$

where s_i is the larger of n_i and m_i.

Problem 12

Show that if $\gcd(a, b) = 1$, then $lcm(a, b) = ab$.
In general, show that:

$$lcm(a, b) = \frac{ab}{\gcd(a, b)}$$

Proof. We prove the general case first.

Let $a = \prod_{i=1}^{r} p_i^{n_i}$ and $b = \prod_{i=1}^{r} p_i^{m_i}$. So

$$ab = \prod_{i=1}^{r} p_i^{n_i+m_i}.$$

Now inspecting the ith prime in ab we get $p_i^{n_i+m_i}$. Then looking at the gcd's ith prime we get $p_i^{\min\{n_i,m_i\}}$. Suppose wlog that $n_i \geq m_i$. Then

$$\frac{p_i^{n_i+m_i}}{p_i^{\min\{n_i,m_i\}}} = \frac{p_i^{n_i+m_i}}{p_i^{m_i}} = p_i^{n_i+m_i-m_i} = p_i^{n_i} = p_i^{\max\{n_i,m_i\}}.$$

This is the ith prime factor of the *lcm*. ∎

Proof. Suppose that for each prime p_i, p_i divides a or b but not both. Then for the ith prime factor p_i, either $n_i = 0$ or $m_i = 0$. Then:

$$\frac{p_i^{n_i+m_i}}{p_i^{\min\{n_i,m_i\}}} = \frac{p_i^{n_i+m_i}}{p_i^{0}} = p_i^{n_i+m_i-0} = p_i^{n_i+m_i} = p_i^{\max\{n_i,m_i\}}.$$

∎

Problem 13

Prove that if m is a common multiple of both a and b, then $lcm(a, b) \mid m$.

Proof. Suppose m is a common multiple of both a and b. Then there exist integers l and f such that $m = la$ and $m = fb$. Let the ith prime factor of a, b, l, f be $p_i^{n_i}$, $p_i^{m_i}$, $p_i^{t_i}$, $p_i^{s_i}$ respectively. Then the ith prime factor of m is

$$m = la = p_i^{n_i+t_i}, \quad m = fb = p_i^{m_i+s_i}.$$

Let the ith prime factor of $\text{lcm}(a, b)$ be $p_i^{\max\{n_i,m_i\}}$. Then, in either case, we have

$$n_i + t_i = m_i + s_i \geq \max\{n_i, m_i\}.$$

So each $p_i^{\max\{n_i,m_i\}}$ divides the corresponding prime factor of m. ∎

Problem 18

(a) Show that in Euclid's Algorithm, the remainders are at least halved after two steps. That is $r_{i+2} < 1/2 r_i$.

(b) Use part a to find the maximum number of steps required for Euclid's algorithm. (Figure this in terms of the maximum of a and b).

Proof. Theorem 2.3 shows that the remainders form a strictly decreasing sequence of integers. Three steps of the algorithm are shown below.

$$\begin{aligned} \text{step 1: } b_{n-2} &= a_{n-2} \cdot q_{n-2} + r_{n-2} \\ \text{step 2: } b_{n-1} &= a_{n-1} \cdot q_{n-1} + r_{n-1} \\ \text{step 3: } b_n &= a_n \cdot q_n + r_n \end{aligned}$$

Now for the ith iteration $b_i = a_{i-1}$ and $a_i = r_{i-1}$. Then:

$$\begin{aligned}\text{step 1: } b_{n-2} &= a_{n-2} \cdot q_{n-2} + r_{n-2}\\ \text{step 2: } a_{n-2} &= r_{n-2} \cdot q_{n-1} + r_{n-1}\\ \text{step 3: } r_{n-2} &= r_{n-1} \cdot q_n + r_n\end{aligned}$$

Notice, in step 3, a larger q_n implies a smaller r_n. So in the worst case $q_n = 1$. So $r_{n-2} = r_{n-1} + r_n \iff r_n = r_{n-2} - r_{n-1}$. Now since $r_n < r_{n-1}$ then $r_{n-2} - r_{n-1} < r_{n-1} \iff r_{n-2} < 2r_{n-1}$. So $\frac{1}{2}r_{n-2} < r_{n-1}$. Now since $r_n < r_{n-2} - r_{n-1}$ then $r_n < r_{n-2} - \frac{1}{2}r_{n-2} = \frac{1}{2}r_{n-2}$. ∎

Solution 18 (b):

Let $c = \max\{a, b\}$. From part (a), we know that after every two steps, the remainder is at most half of the remainder two steps before:

$$r_{i+2} < \frac{1}{2}r_i$$

Let k be the number of "two-step pairs" needed for the remainder to drop below 1. Then

$$\frac{c}{2^k} < 1 \implies 2^k > c \implies k > \log_2 c$$

Since each k corresponds to two iterations, the maximum number of iterations of Euclid's algorithm is

$$\text{max steps} \leq 2k \leq 2\log_2 c$$

Problem 19

Recall from Excersize 1.13 the definition of the binomial coefficient $\binom{n}{k}$. Suppose that p is a positive prime integer, and k is an integer with $1 \leq k \leq p-1$. Prove that p divides binomial coefficient $\binom{p}{k}$.

Proof. By Exercise 1.13, we know that $\binom{p}{k} \in \mathbb{Z}$. Using the factorial definition:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k \cdot (k-1)!(p-k)!} = \frac{p}{k}\binom{p-1}{k-1}.$$

Since p is prime and $1 \leq k \leq p-1$, we have $\gcd(p, k) = 1$, so k divides $\binom{p-1}{k-1}$. Therefore, p divides $\binom{p}{k}$. ∎

3 Modular Arithmetic

Problem 2

Determine the elements of $\mathbb{Z}_{15}$ that have multiplicative inverses. Give an example of an equation of the form $[a]X = [b]$ ($[a] \neq 0$) that has no solution in $\mathbb{Z}_{15}$.

Solution

	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
[0]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[1]	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
[2]	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
[3]	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
[4]	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
[5]	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
[6]	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
[7]	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
[8]	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
[9]	0	9	3	12	6	0	9	3	12	6	0	9	3	12	6
[10]	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
[11]	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
[12]	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
[13]	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
[14]	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Elements with multiplicative inverses are [1],[2],[4],[7],[8],[11],[13], and [14].

Example of an equation of the form $[a]X = [b]$ ($[a] \neq 0$) that has no solution.

$$[3]X = [5]$$

Problem 4

Find an example in $\mathbb{Z}_6$ where $[a][b] = [a][c]$, but $[b] \neq [c]$. How is this related to the existence of multiplicative inverses in $\mathbb{Z}_6$?

Example where $[a][b] = [a][c]$, but $[b] \neq [c]$:

$$[2][2] = [2][5] = [4]$$

You cannot assume that if $[a][b] = [a][c]$ then $[b] = [c]$. This is only true if $[a]$ has a multiplicative inverse.

Problem 5

If $\gcd(a, b) = 1$ then the GCD identity 2.4 garuntees that there exists integers u and v such that $1 = au + mv$. Show that in this case, $[u]_m$ is the multiplicate inverse of $[a]_m$ in $\mathbb{Z}_m$.

Proof. By Theorem 3.2 if $x - y = km$ for some integer k then x,y are in the same residue (mod m). Now $1 = au + mv \iff au = -mv + 1$. Then $x - y = (-mv + 1) - 1 = (-v)m$. Thus $[au]_m = [1]_m$ and therefore $[a]_m \cdot [u]_m = [1]$. ∎

Problem 6

Now use essentially the reverse of the argument from Excersize 5 to show that if $[a]$ has a multiplicative inverse in $\mathbb{Z}_m$, then $\gcd(a, m) = 1$.

Proof. Suppose $[a]_m$ has a multiplicative inverse $[b]_m$ in $\mathbb{Z}_m$. Then $[a] \cdot [b] = [ab] = [1]$. By Theorem 3.2, $ab - 1 = km$. But $ab - km = 1$ so $ab + m(-k) = 1$. Therefore $\gcd(a, m) = 1$. ∎

Problem 7

According to what you have shown in Excersize 5 and 6, which elements of $\mathbb{Z}_{24}$ have multiplicative inverses? What are the inverses for each of those elements? (The answer is somewhat suprising.)

Solution:

The following have multiplicate inverses in $\mathbb{Z}_{24}$.

1. $[1]_{24}$
2. $[5]_{24}$
3. $[7]_{24}$
4. $[11]_{24}$
5. $[13]_{24}$
6. $[17]_{24}$
7. $[19]_{24}$
8. $[23]_{24}$

Problem 9

Prove that the multiplication on $\mathbb{Z}_m$ as defined in the text is well defined, as claimed in Section 3.2.

Proof. Consider $[a]$ and $[b]$. Let x, y be elements in $[a]$ and b, c be elements in $[b]$. We need to show $[xb] = [yc]$. But $x, y \in [a]$ implies $x - y = k_1 m$ for some integer k_1. Also $b, c \in [b]$ implies $b - c = k_2 m$ for some integer k_2. Then:

$$\begin{aligned} & xb - yc \\ =&(k_1 m + y)(k_2 m + c) - yc \\ =&k_1 k_2 m^2 + k_1 mc + k_2 my + yc - yc \\ =&k_1 k_2 m^2 + k_1 mc + k_2 my \\ =&m(k_1 k_2 m + k_1 c + k_2 y) \end{aligned}$$

Showing that $[xb] = [yc]$ ∎

Problem 10

Prove that if all non-zero $\mathbb{Z}_m$ have multiplicative inverses, then multiplicative cancellation holds: that is, if $[a][b] = [a][c]$, then $[b] = [c]$.

Proof. Suppose all non-zero $\mathbb{Z}_m$ have multiplicative inverses. Let $[t]$ be the multiplicative inverse of $[a]$. Then $[a][b] = [a][c] \iff [t][a][b] = [t][a][c] \iff [b] = [c]$. ∎

Problem 13

In the integers, the equation $x^2 = a$ has a solution only when a is a positive perfect square or zero. For which $[a]$ does the equation $[X]^2 = [a]$ have a solution in $\mathbb{Z}_7$? What about in $\mathbb{Z}_8$? What about in $\mathbb{Z}_9$?

Solution:

Elements with square roots in $\mathbb{Z}_7$:

$$[0], [1], [2], [4]$$

Elements with square roots in $\mathbb{Z}_8$:

$$[0], [1], [4]$$

Elements with square roots in $\mathbb{Z}_9$:

$$[0], [1], [4], [7]$$

Problem 14

Explain what $a \equiv b (mod\ 1)$ means.

Solution:

It means when elements in $[a]$ and $[b]$ are divided by 1 the remainder is equivalent. Of course this is true for any a and b since $\frac{a}{1} = a$ and $\frac{b}{1} = b$. So $[a] = [b] = \mathbb{Z}$.

4 Polynomials with Rational Coefficients

Problem 2

Divide the polynomial $x^2 - 3x + 2$ by the polynomial $2x + 1$, to obtain a quotient and remainder as garunteed by the Division Theorem 4.2. Note that although $x^2 - 3x + 2$ and $2x + 1$ are elements of $\mathbb{Z}[x]$, the quotient and remainder are not. Argue that this means that there is not Division Theorem for $\mathbb{Z}[x]$.

Solution:

When $x^2 - 3x + 2$ is divided by $2x + 1$, the quotient is $\frac{1}{2}x - \frac{7}{4}$ and the remainder is $\frac{15}{4}$. To verify:

$$\begin{aligned}(2x+1)\left(\frac{1}{2}x - \frac{7}{4}\right) + \frac{15}{4} &= x^2 - \frac{7}{2}x + \frac{1}{2}x - \frac{7}{4} + \frac{15}{4} \\ &= x^2 - 3x + 2\end{aligned}$$

Clearly, in this example the remainder is not in $\mathbb{Z}[x]$. Therefore, the Division Theorem does not hold in $\mathbb{Z}[x]$. Moreover, the quotient and remainder are unique as guaranteed by the Division Theorem in $\mathbb{Q}[x]$.

Problem 3

By Corollary 4.4 we know that a third-degree polynomial in $\mathbb{Q}[x]$ has at most three roots. Give four examples of third-degree polynomials in $\mathbb{Q}[x]$ that have 0, 1, 2, and 3 roots, respectively; justify your assertions. (Recall that here a root must be a rational number!)

1. 0 roots: $x^3 - 2 = 0$. x would have to satisfy $x^3 = 2$. Clearly no integer cubed equals 2 (so $n = 1$ is impossible). Suppose there exists a rational number in lowest terms $x = \frac{m}{n}$ with $|n| > 1$. Then $(\frac{m}{n})^3 = 2 \iff m^3 = 2n^3$. But this implies $n^3 \mid m^3$, so $n \mid m$, which contradicts that $\gcd(m, n) = 1$. Thus there is no rational root.
2. 1 root: $(x - 0)(x - 0)(x - 0) = 0$. Justification is obvious by root theorem.
3. 2 roots: $(x - 1)(x - 1)(x - 2) = 0$. Justification is obvious by root theorem.
4. 3 roots: $(x - 1)(x - 2)(x - 3) = 0$. Justification is obvious by root theorem.

Problem 4

Your example in the previous exercise of a third-degree polynomial with exactly 2 roots had one repeated root; that is, a root a where $(x-a)^2$ is a factor of the polynomial. (Roots may have multiplicity greater than two of course.) Why can't a third-degree polynomial in $\mathbb{Q}[x]$ have exactly 2 roots where neither is a multiple root.

Proof. Let f be a degree 3 polynomial with two roots, a, b such that $a \neq b$. We can express f in the form

$$f = (x-a)(x-b)l$$

where $l = (x-c)$ is another linear factor. If $c \neq a$ and $c \neq b$, then f has three distinct roots a, b, c, contradicting that f has only two roots. Therefore, $c = a$ or $c = b$, meaning one of the roots is repeated. ∎

Problem 6

Suppose that $f \in \mathbb{Q}[x]$, $q \in \mathbb{Q}$, and $deg(f) > 0$. Use the Root Theorem 4.3 to prove that the equation $f(x) = q$ has at most finitely many solutions.

Proof. Solving $f(x) = q$ is equivalent to solving $l = f - q = 0$. Now $\deg(l) = \deg(f)$ since $\deg(f) > \deg(q)$. By the Root Theorem, every root divides l, reducing its degree by 1. Since $\deg(l)$ is finite, the number of roots is finite. ∎

Problem 8

Prove Theorem 4.7: the GCD identity for $\mathbb{Q}[x]$. Use Euclid's Algorithm 4.5, and the relationship we know between the gcd produced by the algorithm and an arbitrary gcd (Theorem 4.6).

Theorem 1 (GCD Identity 4.7)**.** *If d is a gcd of polynomials f and g, then there exists polynomials a and b so that $d = af + bg$.*

Proof. Let $f, g \in \mathbb{Q}[x]$. By 4.5, there exists a last nonzero remainder r_{n-1} such that $r_{n-2} = q_{n-1}r_{n-1}$ and $r_{n-1} \neq 0$. This remainder r_{n-1} is the $\gcd(f, g)$. From the division steps in the algorithm, each remainder can be expressed as a linear combination of f and g. Thus there exist polynomials $a, b \in \mathbb{Q}[x]$ such that $r_{n-1} = af + bg$. By Theorem 4.6, any other gcd of f and g differs from r_{n-1} by a nonzero rational constant. Therefore, every gcd of f and g in $\mathbb{Q}[x]$ can be expressed as a linear combination of f and g. ∎

Problem 9

One can also prove the GCD identity for $\mathbb{Q}[x]$ with an argument similar to the existential proof of the GCD identity for integers, found in Section 2.3. Try this approach.

Proof. Consider the set of all linear combinations of the polynomials f, g:

$$S = \{fa + gb \,:\, a, b \in \mathbb{Q}[x]\}$$

We must show the $\gcd(f, g)$ belongs to this set. By the Well-ordering Principle, S contains an element d which has the smallest positive degree. Since $d \in S$:

$$d = fa_0 + gb_0$$

For some $a_0, b_0 \in \mathbb{Q}[x]$. Applying the Division Theorem to d, f we get $f = dq + r$. We now show $r = 0$. But:

$$r = f - dq = f - (fa_0 + gb_0)q = f(1 - qa_0) + g(-qb_0)$$

So $r \in S$. Because $\deg(r) < \deg(d)$, and d has the smallest degree of S, we must have $r = 0$. A similar argument shows $d \mid g$.

Now suppose c divides both f and g. Then $f = nc$ and $g = mc$ for some $n, m \in \mathbb{Q}[x]$. Then any linear combination of f and g is also a multiple of c:

$$fa + gb = nca + mcb = c(na + mb)$$

So $c \mid d$. Thus d is the gcd of f and g. ∎

Problem 10

We say that $p \in \mathbb{Q}[x]$ has a multiplicative inverse if there exists $q \in \mathbb{Q}[x]$ such that $pq = 1$. Prove that $p \in \mathbb{Q}[x]$ has a multiplicative inverse if and only if $\deg(p) = 0$.

Proof. ($\rightarrow$) Suppose $p \in \mathbb{Q}[x]$ has a multiplicative inverse. Let q be the multiplicative inverse of p such that $pq = 1$. Clearly $q \neq 0$. If $\deg(p) > 0$ then $\deg(pq) > 0$, but $\deg(pq) = \deg(1) = 0$. Thus $\deg(p) = 0$.

($\leftarrow$) Suppose $\deg(p) = 0$. It follows that $p \in \mathbb{Q}$. Then let $a, b \in \mathbb{Z}$ such that $p = \frac{a}{b}$. We know $a \neq 0$ since $\deg(p) \neq -\infty$. Let $q = \frac{b}{a}$, then $pq = \frac{a}{b} \cdot \frac{b}{a} = 1$. ∎

Problem 11

Suppose that $g \in \mathbb{Q}[x]$, and g divides all elements of $[Q][x]$. Prove that g is a non-zero constant polynomial.

Proof. Clearly $g \neq 0$ since division by 0 is undefined. Suppose, for contradiction, that g is non-constant. That is, $\deg(g) > 0$. Consider $f \in \mathbb{Q}[x]$ such that $f \neq 0$ and $\deg(f) < \deg(g)$. Since $g \mid f$, there exists $c \in \mathbb{Q}[x]$ such that $f = c \cdot g$. But $\deg(f) < \deg(g)$ and $\deg(f) = \deg(c) + \deg(g) \geq \deg(g)$, a contradiction. Thus g is a non-zero constant polynomial. ∎

Problem 12

Find two different polynomials in $\mathbb{Z}_3[x]$ that are equal as functions from $\mathbb{Z}_3 = \mathbb{Z}_3$.

Proof. Let $f(x) = x^3$ and $g(x) = x$. Clearly as polynomials $f \neq g$. Now check each $a \in \mathbb{Z}_3$:

$$0^3 \equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 2 \pmod 3.$$

Thus $f(a) \equiv g(a) \pmod 3$ for all $a \in \mathbb{Z}_3$, so f and g are equal as functions. ∎

Problem 13

Find a non-zero polynomial in $\mathbb{Z}_4[x]$ for which $f(a) = 0$, for all $a \in \mathbb{Z}_4$.

Proof. Let $f(x) = 2x^2 + 2x^4 \in \mathbb{Z}_4[x]$. Now check each element in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$:

$$\begin{aligned}
f(0) &= 2 \cdot 0^2 + 2 \cdot 0^4 = 0, \\
f(1) &= 2 \cdot 1^2 + 2 \cdot 1^4 = 2 + 2 = 4 \equiv 0 \pmod 4, \\
f(2) &= 2 \cdot 2^2 + 2 \cdot 2^4 = 8 + 32 = 40 \equiv 0 \pmod 4, \\
f(3) &= 2 \cdot 3^2 + 2 \cdot 3^4 = 18 + 162 = 180 \equiv 0 \pmod 4.
\end{aligned}$$

Therefore $f(a) = 0$ for all $a \in \mathbb{Z}_4$, but $f(x)$ is not the zero polynomial. ∎

5 Factorization of Polynomials

Problem 1

Prove Theorem 5.1: A polynomial in $\mathbb{Q}[x]$ of degree greater than zero is either irreducible or the product of irreducibles.

Proof. Let f be a polynomial with degree greater than 0. We proceed by induction on the degree of f.

(**Base Case**) A polynomial of degree one is irreducible.

(**Induction Step**) Suppose the theorem holds for all polynomials of degree $m < n$. If f of degree n is irreducible, we are done. Suppose f is not irreducible; then $f = l \cdot g$ where $l, g \in \mathbb{Q}[x]$ and $\deg(l), \deg(g) < \deg(f)$. By the induction hypothesis, l and g can be expressed as a product of irreducible polynomials. Therefore, f can also be expressed as a product of irreducibles. ∎

Problem 2

Prove Theorem 5.2: A polynomial in $\mathbb{Q}[x]$ is irreducible if and only if it is prime.

Proof. Let f be an arbitrary polynomial in $\mathbb{Q}[x]$.

($\rightarrow$) Suppose f is irreducible and $f \mid lg$. Furthermore, suppose f does not divide l. We must show that $f \mid g$. Suppose that d is a common divisor of f and l. Then, because f is irreducible, d must be equal to f or a unit. Because f does not divide l, it must be that $\gcd(f, l) = 1$. So by the GCD identity there exist $x, y \in \mathbb{Q}[x]$ such that $1 = lx + fy$. Multiplying both sides by g gives

$$g = lgx + fgy.$$

Since f divides both terms on the right-hand side, it follows that $f \mid g$, as required.

($\leftarrow$) Suppose f is prime. Furthermore, suppose f has been factored as $f = lg$. Then $f \mid lg$, and so, without loss of generality, $f \mid l$. Thus, $l = fx$, and so $f = fxg$. Cancelling f gives $1 = xg$, and so both x and g must be degree 0 polynomials. This shows that the factorization $f = lg$ is trivial, as required. ∎

Problem 3

Prove Corollary 5.3: If an irreducible polynomial in $\mathbb{Q}[x]$ divides a product $f_1 f_2 f_3 \dots f_n$, then it divides one of f_i.

Proof. Let f be an irreducible polynomial in $\mathbb{Q}[x]$. Furthermore, suppose $f \mid f_1 f_2 f_3 \dots f_n$. We proceed by induction on n.

(**Base Case**) If $f \mid f_1 f_2$, then by the definition of being prime, $f \mid f_1$ or $f \mid f_2$.

(**Induction Step**) Assume the statement holds for $n - 1$; that is, if $f \mid f_1 f_2 \cdots f_{n-1}$, then $f \mid f_i$ for some $i < n$. Now suppose $f \mid f_1 f_2 \cdots f_{n-1} f_n$. Let $c = f_1 f_2 \cdots f_{n-1}$, so $f \mid c f_n$. By the definition of being prime, $f \mid c$ or $f \mid f_n$. By the induction hypothesis, if $f \mid c$, then $f \mid f_i$ for some $i < n$. Thus, in either case, f divides one of the f_i. ∎

Problem 4

Use Gauss's Lemma to determine which of the following are irreducible in $Q[x]$:

$$4x^3 + x - 2, 3x^3 - 6x^2 + x - 2, x^3 + x^2 + x - 1$$

Proof. If $f(x) = 4x^3 + x - 2$ can be factored then one of the factors is of the form $(ax + b)$ where $a, b \in \mathbb{Z}$. The only possible factors are $(4x \pm 1)$, $(4x \pm 2)$, $(2x \pm 2)$, $(2x \pm 1)$, $(x \pm 2)$, $(x \pm 1)$. This implies roots of $\pm\frac{1}{4}, \pm\frac{1}{2}, \pm 2, \pm 1$. By inspection this is not the case. Since f is irreducible in $\mathbb{Z}[x]$ by Gauss's Lemma f is irreducible in $Q[x]$. ∎

Proof. Let $f(x) = 3x^3 - 6x^2 + x - 2$. By inspection $x = 2$ is a root thus by the Root Theorem f is not irreducible in $\mathbb{Q}[x]$. ∎

Proof. If $f(x) = x^3 + x^2 + x - 1$ can be factored then one of the factors is of the form $ax + b$. The only possible factor is $(x \pm 1)$. By inspection this is not the case. Since f is irreducible in $\mathbb{Z}[x]$ by Gauss's Lemma f is irreducible in $Q[x]$. ∎

Problem 6

Prove the Rational Root Theorem 5.6.

Theorem 2 (Ration Root Theorem 5.6)**.** *Suppose that $f = a_0 + a_1 x + \cdots + a_n x^n$ is a polynomial in $\mathbb{Z}[x]$, and $\frac{p}{q}$ is a rational root; that is, p and q are integers, $q \neq 0$, and $f\left(\frac{p}{q}\right) = 0$. We may as well assume also that $gcd(p, q) = 1$. Then q divides the integer a_n, and p divides a_0.*

Proof. We first show $q \mid a_n$. Plugging in $\frac{p}{q}$ shows

$$f\left(\frac{p}{q}\right) = a_0 + a_1\frac{p}{q} + \cdots + a_n\left(\frac{p}{q}\right)^n = 0.$$

Then multiplying through by q^n shows

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0$$

Solving for $a_n p^n$ shows

$$a_n p^n = -a_0 q^n - a_1 p q^{n-1} - a_2 p^2 q^{n-2} - \cdots - a_{n-1} p^{n-1} q$$

Then factoring out q shows

$$a_n p^n = -q(a_0 q^{n-1} + a_1 p q^{n-2} + \cdots + a_{n-1} p^{n-2})$$

Since $\gcd(p, q) = 1$, it follows that $q \nmid p^n$. Thus $q \mid a_n$. We now show $p \mid a_0$. In the previous part it was shown that

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0$$

Solving for $a_0 q^n$ shows

$$a_0 q^n = -(a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n)$$

We can then factor out p so

$$a_0 q^n = -p(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1})$$

Since $\gcd(p, q) = 1$, it follows that $p \nmid q^n$. Thus $p \mid a_0$. ∎

Problem 7

Use the Rational Root Theorem 5.6 to factor

$$2x^3 - 17x^2 - 10x + 9$$

Solution:

Using the Root Theorem we find the following possible roots

$$\text{Candidates} = \{\pm\frac{9}{1}, \pm\frac{9}{2}, \pm\frac{3}{1}, \pm\frac{3}{2}, \pm\frac{1}{1}, \pm\frac{1}{2}\}$$

Inspection shows that 9 and $\frac{1}{2}$ are roots. Dividing $2x^3 - 17x^2 - 10x + 9$ by $(x-9)(x-\frac{1}{2})$ gives us $(2x+2)$. Thus

$$2x^3 - 17x^2 - 10x + 9 = (x-9)(x-\frac{1}{2})(2x+2)$$

Problem 9

Use the Rational Root Theorem 5.6 (applied to $x^3 - 2$) to argue that $\sqrt[3]{2}$ is irrational.

Proof. For contradiction, suppose $\sqrt[3]{2}$ is a rational root for $x^3 - 2$. Since $\sqrt[3]{2}$ is rational it can be expressed as $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$. By the Rational Root Theorem 5.6 it follows that $a \mid -2$ and $b \mid 1$. There exists $k_1, k_2 \in \mathbb{Z}$ such that $-2 = ak_1$ and $1 = bk_2$. Then

$$\sqrt[3]{2} = \frac{\frac{-2}{k_1}}{\frac{1}{k_2}} = \frac{-2k_2}{k_1}$$

It follows that $2 = \frac{-8k_2^3}{k_1^3}$. Multiplying by k_1^3 and dividing by 2 shows that k_1 is even. Rewriting $k_1 = 2k_3$ where $k_3 \in \mathbb{Z}$ we get

$$2 = \frac{-8k_2^3}{(2k_3)^3} \iff 2(2k_3)^3 = -8k_2^3 \iff 16k_3^3 = -8k_2^3.$$

Dividing by 8 shows that k_2 is even, contradicting that $\gcd(a,b) = 1$. ∎

Proof. For contradiction, suppose $\sqrt[3]{2}$ is a rational root of $x^3 - 2$. Then we can write $\sqrt[3]{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$. By the Rational Root Theorem 5.6 any rational root $\frac{a}{b}$ must satisfy $a \mid -2$ and $b \mid 1$. Thus the only possible rational roots are

$$\pm 1, \quad \pm 2.$$

Inspection shows that no combination works. Thus $\sqrt[3]{2}$ is irrational. ∎

Problem 10

Suppose that α is a real number (which might not be rational), and suppose that it is a root of a polynomial $p \in \mathbb{Q}[x]$; that is, $p(\alpha) = 0$. Suppose further that p is irreducible in $\mathbb{Q}[x]$. Prove that p has a minimal degree in the set

$$\mathcal{F} = \{f \in \mathbb{Q}[x] : f(\alpha) = 0 \text{ and } f \neq 0\}$$

Proof. Suppose there exists $g \in \mathbb{Q}[x]$ such that $\deg(g) < \deg(p)$. By the Division Theorem there exists $q, r \in \mathbb{Q}[x]$ such that $p = gq + r$ and $\deg(r) < \deg(g)$. Then

$$0 = p(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha),$$

thus $r(\alpha) = 0$.

Either $\deg(r) = 0$ or $\deg(r) > 0$. Suppose $\deg(r) = 0$, then since $r(\alpha) = 0$, r is the zero polynomial. Since $\deg(p) = \deg(g) + \deg(q)$ and $\deg(g) < \deg(p)$, it follows that $\deg(q) > 0$. Thus p has been factored into two polynomials with degree greater than 0, contradicting the irreducibility of p.

Now, suppose $\deg(r) > 0$. We can repeatedly apply the Division Theorem to form a sequence of decreasing remainders by their degrees.

For example, continuing where we left off, we divide p by r and by the Division Theorem obtain $r_1, q_1 \in \mathbb{Q}[x]$ such that

$$p = rq_1 + r_1.$$

Then $\deg(r_1) < \deg(r) < \deg(g)$.

If at any point a remainder r is a scalar, it must be the zero polynomial and we contradict the irreducibility of p. On the other hand, if the sequence never ends, then we contradict the finiteness of the degree of p. ∎

Problem 12

Construct polynomials of arbitrarily large degree, which are irreducible in $\mathbb{Q}[x]$.

Solution

$$\mathcal{F} = \{f \mid f = x^n - 2\}$$

By Eisenstein's Cirterion all $f \in \mathcal{F}$ are irreducible in $\mathbb{Z}[x]$. By Gauss's Lemma they are irreducible in $\mathbb{Q}[x]$.

Problem 13

(a) Prove that the equation $a^2 = 2$ has no ration solutions; that is, prove that $\sqrt{2}$ is irrational. (This part is a repeat of exercise 2.14.)
(b) Generalize part *a*,k by proving that $a^n = 2$ has no rational solutions, for all positive integers $n \geq 2$.

Proof. Let $p = 2$ and apply Eisenstein's Criterion to $a^2 - 2 = 0$. Clearly 2 is prime, $2 \mid -2$, $2 \nmid 1$, and $2^2 \nmid -2$. Thus there is no rational root. ∎

Proof. Same logic as before. ∎

Problem 14

Let $f \in \mathbb{Z}[x]$ and n an integer. Let g be the polynomial defined by $g(x) = f(x + n)$. Prove that f is irreducible in $\mathbb{Z}[x]$ if and only if g is irreducible in $\mathbb{Z}[x]$.

Proof. Let $y = x - n$, so that $f(x + n) = g(y) = g(x - n)$.

($\rightarrow$) Suppose f is irreducible in $\mathbb{Z}[x]$. For contradiction suppose g is reducible: $g = pl$ where $p, l \in \mathbb{Z}[x]$. Then

$$f(x) = g(x - n) = p(x - n)l(x - n),$$

contradicting the irreducibility of f. Thus g is irreducible in $\mathbb{Z}[x]$.

($\leftarrow$) Suppose g is irreducible in $\mathbb{Z}[x]$. For contradiction suppose f is reducible: $f = pl$ where $p, l \in \mathbb{Z}[x]$. Then

$$g(x) = f(x + n) = p(x + n)l(x + n),$$

contradicting the irreducibility of g. Thus f is irreducible in $\mathbb{Z}[x]$. ∎

Problem 15

(a) Apply Eisenstein's criterion 5.7 to check that the following polynomials are irreducible

$$5x^3 - 6x^2 + 2x - 14 \text{ and } 4x^5 + 5x^3 - 15x + 20$$

(b) Make the substition $x = y + 1$ to the polynomial $x^5 + 5x + 4$ that appears in Example 5.1. Show that the resulting polynomial is irreducible.

(c) Use the same technique as in part b to find a substitution $x = y + m$ so you can conclude the polynomial

$$x^4 + 6x^3 + 12x^2 + 10x + 5$$

is irreducible.
(d) Show that this technique works in general: Prove that if $f(x) \in \mathbb{Z}[x]$, then $f(x)$ is irreducible if and only if $f(y + m)$ is.

Solution (a): Consider $2 \nmid 5$. Also $2 \mid -6, 2, -14$. Finally $2^2 = 4 \nmid -14$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus $5x^3 - 6x^2 + 2x - 14$ is irreducible in $\mathbb{Z}[x]$.

Consider $5 \nmid 4$. Also $5 \mid 5, -15, 20$. Finally $5^2 = 25 \nmid 20$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus $4x^5 + 5x^3 - 15x + 20$ is irreducible in $\mathbb{Z}[x]$.

Solution (b): Substituting $x = y + 1$ into $x^5 + 5x + 4$ gives

$$(y + 1)^5 + 5(y + 1) + 4 = y^5 + 5y^4 + 10y^3 + 10y^2 + 10y + 10.$$

Consider $5 \nmid 1$. Also $5 \mid 5, 10, 10, 10, 10$. Finally $5^2 = 25 \nmid 10$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus the polynomial is irreducible in $\mathbb{Z}[y]$, and so $x^5 + 5x + 4$ is irreducible in $\mathbb{Z}[x]$.

Solution (c): Substituting $x = y + 1$ into $x^4 + 6x^3 + 12x^2 + 10x + 5$ gives

$$(y + 1)^4 + 6(y + 1)^3 + 12(y + 1)^2 + 10(y + 1) + 5 = y^4 + 10y^3 + 36y^2 + 56y + 34.$$

Consider $2 \nmid 1$. Also $2 \mid 10, 36, 56, 34$. Finally $2^2 = 4 \nmid 34$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus $y^4 + 10y^3 + 36y^2 + 56y + 34$ is irreducible in $\mathbb{Z}[y]$.

Proof. ($\longrightarrow$) Let $x = y + m$. Suppose $f(x)$ is irreducible. For contradiction, suppose $f(y + m)$ is reducible. Thus $f(y + m) = g(y)\,l(y)$ for some $g(y), l(y) \in \mathbb{Z}[y]$. But $x = y + m$, so $f(x) = g(x - m)\,l(x - m)$. Thus $f(x)$ is reducible, which is a contradiction.

($\longleftarrow$) Let $x = y + m$. Suppose $f(y + m)$ is irreducible. For contradiction, suppose $f(x)$ is reducible. Thus $f(x) = g(x)\,l(x)$ for some $g(x), l(x) \in \mathbb{Z}[x]$. But $x = y + m$, so $f(y + m) = g(y + m)\,l(y + m)$. Thus $f(y + m)$ is reducible, which is a contradiction. ∎

Problem 16

Prove Theorem 5.7 (Eisenstein's criterion).

Theorem 3 (Eisenstein's Criterion)**.** *Suppose that $f \in \mathbb{Z}[x]$, and*

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

Let p be a prime integer, and suppose that

1. *p divides a_k, for $0 \leq k < n$,*
2. *p does not divide a_n, and*
3. *p^2 does not divide a_0*

Then f is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose for contradiction that f is reducible. Then there exist polynomials $g, l \in \mathbb{Z}[x]$ such that $f = gl$:

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = gl.$$

Now p either divides the constant term of g or l; otherwise it would not divide the constant term of f. Furthermore, if p divides the constant term of both, then p^2 would divide the constant term of f, which is

impossible. Suppose w.l.o.g. that p divides the constant term of g and p does not divide the constant term of l. The constant term of l cannot be zero; otherwise the constant term of f would be zero.

Now consider the first coefficient b_j of g with $j > 0$ that is not divisible by p. This term exists since coefficientof largest degree term of g is not divisible by p. Let c be the constant term of l, so $p \nmid c$. Then the product $b_j c$ contributes to the coefficient a_j of f. Since $p \nmid b_j$ and $p \nmid c$, it follows that $p \nmid b_j c$.

Any other contributions to a_j come from products of terms of g and l where at least one factor is divisible by p, so those terms are divisible by p. Thus the coefficient a_j of f is

$$a_j = b_j c + (\text{terms divisible by } p),$$

which is not divisible by p, contradicting the assumption that p divides a_k for all $0 \leq k < n$. ∎

Problem 17

Let p be a positive prime integer. Then the polynomial

$$\phi_p = \frac{x^p - 1}{x - 1}$$

is called a **cyclotomic polynomial**.
(a) Write out, in the usual form for a polynomial, the cyclotomic polynomials for the first three primes.
(b) Prove that all cyclotomic polynomials ϕ_p are irreducible over $\mathbb{Z}[x]$, using Eisenstein's criterion 5.7 and Exercise 15d for $m = 1$.

Solution (a):

$$p = 2, \frac{x^2 - 1}{x - 1} = \frac{(x-1)(x+1)}{x-1} = x + 1$$

$$p = 3, \frac{x^3 - 1}{x - 1} = \frac{(x-1)(x^2+x+1)}{x-1} = x^2 + x + 1$$

$$p = 5, \frac{x^5 - 1}{x - 1} = \frac{(x-1)(x^4+x^3+x^2+x+1)}{x-1} = x^4 + x^3 + x^2 + x + 1$$

Proof. Let $x = y + 1$. Let p be an arbitrary prime. Then consider

$$\frac{(y+1)^p - 1}{(y+1) - 1} = \frac{(y+1)^p - 1}{y}$$

We can re-express the numerator using the binomial theorem

$$(y+1)^p = \sum_{k=0}^{p} \binom{p}{k} y^{p-k} 1^k = \sum_{k=0}^{p} \binom{p}{k} y^{p-k}$$

Substituting into the fraction gives

$$\frac{(y+1)^p - 1}{y} = \frac{\sum_{k=0}^{p} \binom{p}{k} y^{p-k} - 1}{y}$$

Multiplying numerator and denominator by y^{-1}/y^{-1} gives

$$\frac{\sum_{k=0}^{p} \binom{p}{k} y^{p-k} - 1}{y} \cdot \frac{y^{-1}}{y^{-1}} = \sum_{k=0}^{p} \binom{p}{k} y^{p-k-1} - y^{-1}$$

Now we re-express this summation and extract the cases $k = 0, p-1, p$ to show

$$\sum_{k=0}^{p}\binom{p}{k}y^{p-k-1} - y^{-1} = y^{p-1} + \sum_{k=1}^{p-2}\binom{p}{k}y^{p-k-1} + \binom{p}{p-1}y^0 + \binom{p}{p}y^{-1} - y^{-1} = y^{p-1} + \sum_{k=1}^{p-2}\binom{p}{k}y^{p-k-1} + \binom{p}{p-1}$$

Now y^{p-1} is the term with the highest degree and its coefficient is 1. Clearly $p \nmid 1$, satisfying part (a) of Eisenstein's criterion. Furthermore, by Chapter 2 Problem 19, since p is a positive prime integer and k is an integer with $1 \leq k \leq p-1$, we have $p \mid \binom{p}{k}$. Additionally, $p \mid \binom{p}{p-1} = p$. Thus part (b) of Eisenstein's criterion is satisfied. Now, the constant term of $\frac{(y+1)^p-1}{y}$ is p. Since $a_0 = p < p^2$, we have $p^2 \nmid a_0$, satisfying part (c) of Eisenstein's criterion. By Problem 15 part d, it follows that all cyclotomic polynomials ϕ_p are irreducible over $\mathbb{Z}[x]$. ∎

6 Rings

Problem 1

Show that in a ring, $0a = a0 = 0$.

Proof. Let R be a ring and a be an arbitrary element in R. Then

$$\begin{aligned}
0a &= 0a + 0 && \text{Rule 3}\\
&= 0a + (0a + (-0a)) && \text{Rule 4}\\
&= (0a + 0a) + (-0a) && \text{Rule 2}\\
&= ((0+0)a) + (-0a) && \text{Rule 6}\\
&= 0a + (-0a) && \text{Rule 3}\\
&= 0 && \text{Rule 3}
\end{aligned}$$

Similarly

$$\begin{aligned}
a0 &= a0 + 0 && \text{Rule 3}\\
&= a0 + (a0 + (-a0)) && \text{Rule 4}\\
&= (a0 + a0) + (-a0) && \text{Rule 2}\\
&= (a(0+0)) + (-a0) && \text{Rule 6}\\
&= a0 + (-a0) && \text{Rule 3}\\
&= 0 && \text{Rule 3}
\end{aligned}$$

Thus $a0 = 0a = 0$. ∎

Problem 2

Prove part d of Theorem 6.1: Show that in a ring the additive identity is unique, by supposing 0 and $0'$ satisfy Rule 3 and proving that $0 = 0'$.

Proof. Let R be a ring and suppose there exists $0 \in R$ and $0' \in R$ such that for all $a \in R$, $a + 0 = a$ and $a + 0' = a$. Then $a + 0 = a = a + 0'$. By Additive Cancellation $0 = 0'$. ∎

Problem 3

Show that in a ring $(-a)b = a(-b) = -(ab)$.

Proof. Let R be a ring and $a, b \in R$. Then

$$\begin{aligned}
0 = (a + (-a))b &\iff 0 = ab + (-a)b && \text{Rule 6}\\
&\iff -(ab) + 0 = -(ab) + (ab + (-a)b)\\
&\iff -(ab) = -(ab) + (ab + (-a)b) && \text{Rule 3}\\
&\iff -(ab) = (-(ab) + ab) + (-a)b && \text{Rule 2}\\
&\iff -(ab) = 0 + (-a)b && \text{Rule 4}\\
&\iff -(ab) = (-a)b + 0 && \text{Rule 1}\\
&\iff -(ab) = (-a)b && \text{Rule 3}
\end{aligned}$$

Also

$$\begin{aligned}
0 = a(b + (-b)) &\iff 0 = ab + a(-b) && \text{Rule 6}\\
&\iff -(ab) + 0 = -(ab) + ((ab) + a(-b))\\
&\iff -(ab) = -(ab) + ((ab) + a(-b)) && \text{Rule 3}\\
&\iff -(ab) = (-(ab) + (ab)) + a(-b) && \text{Rule 2}\\
&\iff -(ab) = 0 + a(-b) && \text{Rule 4}\\
&\iff -(ab) = a(-b) + 0 && \text{Rule 1}\\
&\iff -(ab) = a(-b) && \text{Rule 3}
\end{aligned}$$

Thus $(-a)b = a(-b) = -(ab)$. ∎

Problem 4

Show that in a ring $(-a)(-b) = ab$.

Proof.

$$\begin{aligned}
(-a)(-b) + -(ab) &= a(-(-b)) + a(-b) && \text{Rule 6}\\
&= a((-(-b)) + (-b)) && \text{Rule 2}\\
&= a \cdot 0 && \text{Rule 4}\\
&= 0 && \text{Rule 3}
\end{aligned}$$

Thus $(-a)(-b) = ab$. ∎

Problem 5

Prove the following facts about subtraction in a ring R, where $a, b, c \in R$.
(a) $a - a = 0$.
(b) $a(b - c) = ab - ac$.
(c) $(b - c)a = ba - ca$.

Proof. Let R be a ring and $a, b, c \in R$. Then $a - a = a + (-a) = 0$ Rule 4. Also, $a(b - c) = a(b + (-c)) = ab + a(-c)$ Rule 6. Then, $ab + a(-c) = ab + -(ac)$ Problem 3 $= ab - ac$. Similarly, $(b - c)a = (b + (-c))a = ba + (-c)a$ Rule 6. Then, $ba + (-c)a = ba + -(ca)$ Problem 3 $= ba - ca$. ∎

Problem 8

We generalize Exercises 6 and 7: Let R be any commutative ring (other than the zero ring). Define $M_2(R)$ as the set of 2×2 matrices with entries from R. Show that $M_2(R)$ is a ring which is not commutative. (Note that for the most part the proofs in Exercises 6 and 7 life over without change.)

Proof. Let R be a ring and

$$a, b, c, e, f, g, h, i, j, k, l \in R$$

We first show associativity with respect to +.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(R), \begin{bmatrix} c & f \\ g & h \end{bmatrix} \in M_2(R) \text{ and } \begin{bmatrix} i & j \\ k & l \end{bmatrix} \in M_2(R)$$

Then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} c & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+c & b+f \\ c+g & d+h \end{bmatrix} = \begin{bmatrix} c+a & f+b \\ g+c & h+d \end{bmatrix} = \begin{bmatrix} c & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We now show associativity with respect to +.

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} c & f \\ g & h \end{bmatrix}\right) + \begin{bmatrix} i & j \\ k & l \end{bmatrix} = \begin{bmatrix} a+c & b+f \\ c+g & d+h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} = \begin{bmatrix} (a+c)+i & (b+f)+j \\ (c+g)+k & (d+h)+l \end{bmatrix}$$

$$= \begin{bmatrix} a+(c+i) & b+(f+j) \\ c+(g+k) & d+(h+l) \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} c+i & f+j \\ g+k & h+l \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} c & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right)$$

We now show the existence of an additive inverse.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-a & b-b \\ c-c & d-d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

We now show the existence of the additive identity.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a+0 & b+0 \\ c+0 & d+0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We now show left distributivity.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix} = \begin{bmatrix} a(e+i)+b(g+k) & a(f+j)+b(h+l) \\ c(e+i)+d(g+k) & c(f+j)+d(h+l) \end{bmatrix}$$

$$= \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} + \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} i & j \\ k & l \end{bmatrix}.$$

We now show right distributivity.

$$\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right)\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} (e+i)a+(f+j)c & (e+i)b+(f+j)d \\ (g+k)a+(h+l)c & (g+k)b+(h+l)d \end{bmatrix}$$

$$= \begin{bmatrix} ea+fc & eb+fd \\ ga+hc & gb+hd \end{bmatrix} + \begin{bmatrix} ia+jc & ib+jd \\ ka+lc & kb+ld \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We now show matrix multiplication is not commutative by giving a counterexample. Consider

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 1+6 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 3 & 1 \end{bmatrix}$$

But multiplying the same matrices in the opposite order gives

$$\begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}.$$

Since

$$\begin{bmatrix} 7 & 2 \\ 3 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}$$

matrix multiplication is not commutative. ∎

Let $R = \{0, a, ...\}$ such that $0 \neq a$.

$$A = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix}$$

$$AB = \begin{bmatrix} a^2 & 0 \\ 0 & 0 \end{bmatrix} \neq BA = \begin{bmatrix} 0 & 0 \\ 0 & a^2 \end{bmatrix}$$

Problem 9

Check that Example 6.14 is indeed a ring; that is, let $C[0,1]$ be a set of functions defined from the closed unit interval $[0,1]$ to the real numbers that are continuous. Define the sum and product of two functions point-wise: $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. Show that $C[0,1]$ is a commutative ring. (You may use theorems from calculus).

Proof. Let $x \in [0,1]$ and $f, g, l : [0,1] \longrightarrow \mathbb{R}$. Since $f(x), g(x), l(x) \in \mathbb{R}$ and $\mathbb{R}$ is a ring, standard ring operations (associativity, distributivity, etc.) hold. We first show commutativity over addition

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$$

Next, associativity over addition

$$((f+g)+l)(x) = (f+g)(x) + l(x) = f(x) + g(x) + l(x) = f(x) + (g+l)(x) = (f+(g+l))(x).$$

Existence of additive inverses

$$(f + (-f))(x) = f(x) + (-f(x)) = 0$$

Additive identity

$$(f+0)(x) = f(x) + 0(x) = f(x)$$

Commutativity of multiplication

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$$

Associativity of multiplication

$$((fg)l)(x) = (fg)(x)l(x) = f(x)g(x)l(x) = f(x)(gl)(x) = (f(gl))(x)$$

Distributivity from the left

$$f(g+l)(x) = f(x)(g+l)(x) = f(x)(g(x) + l(x)) = f(x)g(x) + f(x)l(x) = (fg + fl)(x)$$

Distributivity from the right

$$(f+g)l(x) = (f+g)(x)\,l(x) = (f(x) + g(x))l(x) = f(x)l(x) + g(x)l(x) = (fl + gl)(x)$$

∎

Problem 11

Let $\mathbb{C}$ be the complex numbers. That inverse

$$\mathbb{C} = \{a + bi \mid a, b, \in \mathbb{R}\}$$

where i is the square root of -1 (that is, $i \cdot i = 1$). Here

$$(a + bi) + (c + di) = (a + c) + (bi + di)$$

and

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Show that $\mathbb{C}$ is a commutative ring.

Proof. Let $a + bi,\ c + di,\ e + fi \in \mathbb{C}$. Commutativity of addition

$$(a + bi) + (c + di) = (a + c) + (b + d)i = (c + a) + (d + b)i = (c + di) + (a + bi)$$

Associativity of addition

$$((a + bi) + (c + di)) + (e + fi) = (a + c + e) + (b + d + f)i$$

$$= (a + bi) + ((c + di) + (e + fi))$$

Additive identity

$$(a + bi) + 0 = (a + 0) + (b + 0)i = a + bi$$

Additive inverses

$$(a + bi) + (-a - bi) = (a - a) + (b - b)i = 0$$

Commutativity of multiplication

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = (c + di)(a + bi)$$

Associativity of multiplication

$$((a + bi)(c + di))(e + fi) = (a + bi)((c + di)(e + fi))$$

Left distributivity

$$(a + bi)((c + di) + (e + fi)) = (a + bi)((c + e) + (d + f)i)$$

$$= a(c + e) - b(d + f) + (a(d + f) + b(c + e))i$$

$$= (ac - bd) + (ad + bc)i \ + \ (ae - bf) + (af + be)i$$

$$= (a + bi)(c + di) + (a + bi)(e + fi)$$

Right distributivity

$$((a + bi) + (c + di))(e + fi) = ((a + c) + (b + d)i)(e + fi)$$

$$= (a + c)e - (b + d)f + ((a + c)f + (b + d)e)i$$

$$= (ae - bf) + (af + be)i \ + \ (ce - df) + (cf + de)i$$

$$= (a + bi)(e + fi) + (c + di)(e + fi)$$

∎

Problem 15

Verify that 6.10 is a ring. Namely, let R and S be arbitrary rings. Define addition and subtraction appropriately to make $R \times S$ a ring, where $R \times S$ is the set of ordered pairs with the first entry from R and second entry from S. Now generalize this to the set $R_1 \times R_2 \times \cdots R_n$ of n-tuples with entries from the rings R_i. This new ring is called the **direct product** of the rings R_i.

Definition 1. *Let R, S be arbitrary rings. Let $(a,b),(c,d) \in R \times S$. We define $\cdot$ pointwise such that $(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$. Similarly we define $+$ pointwise such that $(a,b)+(c,d) = (a+c, b+d)$.*

Definition 2. *Let R, S be arbitrary rings. Let $(r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_n), (r_1', r_2', \dots, r_n', s_1', s_2', \dots, s_n') \in (R_1 \times R_2 \times \cdots \times R_n) \times (S_1 \times S_2 \times \cdots \times S_n)$. We define $\cdot$ pointwise such that $(r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_n)\cdot(r_1', r_2', \dots, r_n', s_1', s_2', \dots, s_n') = (r_1 \cdot r_1', r_2 \cdot r_2', \dots, r_n \cdot r_n', s_1 \cdot s_1', s_2 \cdot s_2', \dots, s_n \cdot s_n')$. Similarly we define $+$ pointwise such that $(r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_n) + (r_1', r_2', \dots, r_n', s_1', s_2', \dots, s_n') = (r_1 + r_1', r_2 + r_2', \dots, r_n + r_n', s_1 + s_1', s_2 + s_2', \dots, s_n + s_n')$.*

Proof. Let R and S be arbitrary rings. Let $(a,b),(c,d),(e,f) \in R \times S$.

(**Rule 1**)

$$(a,b) + (c,d) = (a+c, b+d) \qquad = (c+a, d+b) = (c,d) + (a,b)$$

(**Rule 2**)

$$\begin{aligned}(a,b) + [(c,d) + (e,f)] &= (a,b) + (c+e, d+f) \\ &= (a + (c+e), b + (d+f)) \\ &= ((a+c) + e, (b+d) + f) \\ &= (a+c, b+d) + (e,f) \\ &= [(a,b) + (c,d)] + (e,f)\end{aligned}$$

(**Rule 3**)

$$\begin{aligned}(a,b) + (0,0) &= (a+0, b+0) \\ &= (a,b)\end{aligned}$$

(**Rule 4**)

$$\begin{aligned}(a,b) + (-a,-b) &= (a-a, b-b) \\ &= (0,0)\end{aligned}$$

(**Rule 5**)

$$\begin{aligned}(a,b)[(c,d)(e,f)] &= (a,b)(ce, df) \\ &= (a(ce), b(df)) \\ &= ((ac)e, (bd)f) \\ &= (ac, bd)(e,f) \\ &= [(a,b)(c,d)](e,f)\end{aligned}$$

(**Rule 6 Left**)

$$\begin{aligned}(a,b)[(c,d) + (e,f)] &= (a,b)(c+e, d+f) \\ &= (a(c+e), b(d+f)) \\ &= (ac + ae, bd + bf) \\ &= (ac, bd) + (ae, bf) \\ &= (a,b)(c,d) + (a,b)(e,f)\end{aligned}$$

(**Rule 6 Right**)

$$\begin{aligned}[(a,b)(c,d)](e,f) &= (a+c, b+d)(e,f) \\ &= ((a+c)e, (b+d)f) \\ &= (ae + ce, bf + df) \\ &= (ae, bf) + (ce, df) \\ &= (a,b)(e,f) + (c,d)(e,f)\end{aligned}$$

We proceed via induction to prove the direct product of an arbitrary number of rings is indeed a ring. The proceeding part of this proof shows the base case. Suppose it holds for some $R_1 \times R_2 \times \cdots \times R_n$ where $n \in \mathbb{N}$. Consider $R_1 \times R_2 \times \cdots \times R_n \times R_{n+1}$. Now, $R_1 \times R_2 \times \cdots \times R_n$ is a ring and R_{n+1} is a ring and our proceeding part of the proof works for arbitrary rings thus $R_1 \times R_2 \times \cdots \times R_n \times R_{n+1}$ is a ring. ∎

Problem 16

Find an example of $M_2(\mathbb{Z})$ to show that $(a+b)^2$ is not necessarily equal to $a^2 + 2ab + b^2$. (Recall that $2ab = ab + ab$.) What is the correct expansion of $(a+b)^2$ for an arbitrary ring? What can you say of the ring is commutative.

Solution:

$$(a+b)^2 = \left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)^2 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1\cdot 1 + 2\cdot 2 & 1\cdot 2 + 2\cdot 1 \\ 2\cdot 1 + 1\cdot 2 & 2\cdot 2 + 1\cdot 1 \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix}.$$

$$a^2 + 2ab + b^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^2 + 2\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 5 & 2 \\ 6 & 5 \end{bmatrix}.$$

The correct expansion is $(a+b)^2 = a^2 + ab + ba + b^2$.

If the ring is commutative then $ab = ba$ thus $(a+b)^2 = a^2 + 2ab + b^2$.

Problem 17

(This exercise extends the discussion of Exercise 16.) Let R be a commutative ring and $a, b \in R$. Then prove the *binomial theorem* for R, by induction on n: Namely, show that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Proof. (**Base Case:**) Trivial.

(**Induction Step:**) Assume the formula holds for $n-1$, thus:

$$\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} = (x+y)^{n-1}$$

Then:

$$\begin{aligned}
(x+y)^n &= (x+y)^{n-1} \cdot (x+y) \\
&= \left(\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k}\right) \cdot (x+y) \\
&= x \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} + y \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \left(\binom{n-1}{k-1} + \binom{n-1}{k}\right) x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}
\end{aligned}$$

Problem 18

Suppose $a \cdot a = a$ for every element a in a ring R. (Elements a in a ring where $a^2 = a$ are called **idempotent**.)
(a) Show that $a = -a$.
(b) Now show that R is commutative.

Proof. Since every element of R is idempotent, we have $a^2 = a$. Because $a + a \in R$, it is also idempotent, so $(a + a)^2 = a + a$. Expanding using distributivity gives $(a + a)^2 = a^2 + a^2 + a^2 + a^2 = 4a^2$. Substituting $a^2 = a$ yields $4a = 2a$. Subtracting $2a$ from both sides gives $2a = 0$. Thus $a + a = 0$, and therefore $a = -a$. ∎

Proof. Let $a, b \in R$. Since every element is idempotent, we have $(a + b)^2 = a + b$. Expanding the left-hand side gives $(a + b)^2 = a^2 + ab + ba + b^2$. Using $a^2 = a$ and $b^2 = b$, this becomes $a + ab + ba + b = a + b$. Canceling $a + b$ from both sides yields $ab + ba = 0$. From part (a), every element equals its additive inverse, so $ab = -ab = ba$. Hence $ab = ba$, and R is commutative. ∎

Problem 19

Let $S = \{(x_2, x_2, x_3, ...) \mid x_i \in \mathbb{R}\}$, the real-valued sequences. Define addition and multiplication on S coordinate-wise (see Exercise 13 and 14). Show that S is a commutative ring.

Proof. We know from problem 14 that S is a ring. The $\cdot$ operation for the direct product is based on the multiplication of $\mathbb{R}$ which commutes. Thus S is a commutative ring. ∎

Problem 20

Let X be some arbitrary set, an $P(X)$ the set of all subsets of X. In Example 1.1 we proved that if X has n elements, then $P(X)$ has 2^n elements; we are here allowing the possibility that X (and hence $P(X)$) has *infinitely* many elements. Define operations on $P(X)$ as follows, where $a, b \in P(X)$:

$$a + b = (a \cup b) \setminus (a \cap b) \text{ and } ab = a \cap b$$

(Addition here is often called the **symmetric difference** of the two sets a, b.) Prove that $P(X)$ is commutative ring. ($P(X)$ is called the **power set** for the set X.)

Proof. Let $a, b, c \in P(X)$.

(**Rule 1**)
$$a + b = (a \cup b) \setminus (a \cap b) = (b \cup a) \setminus (b \cap a) = b + a.$$

(**Rule 2**)
$$(a + b) + c = a + (b + c).$$

(**Rule 3**)
$$a + \emptyset = (a \cup \emptyset) \setminus (a \cap \emptyset) = a.$$

(**Rule 4**)
$$a + a = (a \cup a) \setminus (a \cap a) = a \setminus a = \emptyset.$$

(**Rule 5**) The intersection is associative thus

$$(ab)c = a(bc).$$

(**Rule 6 Left**)

$$a(b+c) = a \cap \big((b \cup c) \setminus (b \cap c)\big) = (a \cap b) + (a \cap c) = ab + ac.$$

(**Rule 6 Right**)

$$(a+b)c = \big((a \cup b) \setminus (a \cap b)\big) \cap c = (a \cap c) + (b \cap c) = ac + bc.$$

∎

Problem 23

Let R be any commuatative ring. Let $R[x]$ be the collection of polynomials with coefficients from R. Show that $R[x]$ is a ring.

Proof. Since addition and multiplication in $R[x]$ are defined coefficient-wise using the operations in the ring R, and since R satisfies the ring axioms, it follows that $R[x]$ also satisfies the ring axioms. Thus $R[x]$ is a ring. ∎

7 Subrings and Unity

Warmup d

Give examples of the following (or explain why they don't exist):
(a) A commutative subring of a non-commutative ring.
(b) A non-commutative subring of a commutative ring.
(c) A subring without unity, of a ring with unity. (See Exercise 22 for the converse possibility)
(d) A ring (with more than one element) whose only subrings are itself, and the zero subring. *Hint:* Look at an earlier Warm-up Exercise.

Solution (a): The trivial ring.

Solution (b): Does not exist. The elements required are still in the subring thus they commute.

Solution (c): $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ and does not have unity.

Solution (d): The only subring of $\mathbb{Z}_5$ is the trivial ring.

Warmup e

What is the unity of the power set ring $\mathscr{P}(X)$ considered in Exercise 6.20?

Solution: The set X.

Warmup f

What is the unity of the ring $\mathbb{Z} \times \mathbb{Z}$? (See Example 6.9) What about $R \times S$, where R and S are rings with unity? (See Example 6.10.)

Solution: The unity of $\mathbb{Z} \times \mathbb{Z}$ is $(1,1)$. The unity of $R \times S$ is (r,s) where r,s is the unity of R,S respectively.

Problem 2

We generalize Exercise 1: Let $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a,b, \in \mathbb{Z}\}$ where n is some fixed integer (positive or negative). Show that $\mathbb{Z}[\sqrt{n}]$ is a commutative ring by showing it is a subring of $\mathbb{C}$.

Proof. Let $a+b\sqrt{n}, c+d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$. Then $(a+b\sqrt{n})-(c+d\sqrt{n}) = (a-c)+(b-d)\sqrt{n}$. Now, $a-c \in \mathbb{Z}$ and $b-d \in \mathbb{Z}$ thus $\mathbb{Z}[\sqrt{n}]$ is closed under subtraction. Similarly $(a+b\sqrt{n})(c+d\sqrt{n}) = (ac+bdn)+(ad+bc)\sqrt{n}$. Now, $ac+bdn \in \mathbb{Z}$ and $ad+bc \in \mathbb{Z}$ thus $\mathbb{Z}[\sqrt{n}]$ is closed under multiplication. It follows from Theorem 7.1 that $\mathbb{Z}[\sqrt{n}]$ is a subring of $\mathbb{C}$. ∎

Problem 3

Let $\alpha = \sqrt[3]{5}$ and $\mathbb{Z}[\alpha] = \{a+b\alpha+c\alpha^2 \mid a,b,c \in \mathbb{Z}\} \subseteq \mathbb{R}$. Prove that $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{R}$.

Proof. Let $a+b\alpha+c\alpha^2, d+e\alpha+f\alpha^2 \in \mathbb{Z}[\alpha]$. Then $(a+b\alpha+c\alpha^2)-(d+e\alpha+f\alpha^2) = (a-d)+(b-e)\alpha+(c-f)\alpha^2$. Now, $a-d, b-e, c-f \in \mathbb{Z}$ thus $\mathbb{Z}[\alpha]$ is closed under subtraction. Similarly $(a+b\alpha+c\alpha^2)(d+e\alpha+f\alpha^2) = (ad+5bf+5ce)+(ae+bd+5cf)\alpha+(af+be+cd)\alpha^2$. To see this simply note that $\alpha^3 = 5$ and $\alpha^4 = 5\alpha$. Now, $ad+5bf+5ce, ae+bd+5cf, af+be+cd \in \mathbb{Z}$ thus $\mathbb{Z}[\alpha]$ is closed under multiplication. It follows from Theorem 7.1 that $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{R}$. ∎

Problem 4

Show that $m\mathbb{Z}$ is a subring of $n\mathbb{Z}$ if and only if n divides m. (See Example 7.7)

Proof. ($\longrightarrow$) Suppose $m\mathbb{Z}$ is a subring of $n\mathbb{Z}$. If $m = 0$ then clearly $n \mid m$. Therefore, suppose $m \neq 0$. Now, $m\mathbb{Z} \subseteq n\mathbb{Z}$. Thus $m \in n\mathbb{Z}$ since $m \in m\mathbb{Z}$. Therefore there exists $k \in \mathbb{Z}$ such that $m = nk$, so $n \mid m$.

($\longleftarrow$) Suppose n divides m. Let $x, y \in m\mathbb{Z}$. Then $x = mk_1, y = mk_2$, for some $k_1, k_2 \in \mathbb{Z}$. Since $n \mid m$ there exists $k_3 \in \mathbb{Z}$ such that $x = mk_1 = n(k_3k_1) \in n\mathbb{Z}$. Thus $m\mathbb{Z} \subseteq n\mathbb{Z}$. Then $x-y = mk_1 - mk_2 = m(k_1-k_2) \in m\mathbb{Z}$. Thus $m\mathbb{Z}$ is closed under subtraction. Similarly, $xy = (mk_1)(mk_2) = m(k_1mk_2) \in m\mathbb{Z}$. Thus $m\mathbb{Z}$ is closed under multiplication. It follows from Theorem 7.1 that $m\mathbb{Z}$ is a subring of $n\mathbb{Z}$. ∎

Problem 5

(a) Show that $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$.
(b) Let m and n be two positive integers. Show that $m\mathbb{Z} \cap n\mathbb{Z} = f\mathbb{Z}$ where l is the least common multiple of m and n. (See Exercise 2.11.)

Proof. Let x be an arbitrary element in $4\mathbb{Z} \cap 6\mathbb{Z}$. Then $x \in 4\mathbb{Z}$ and $x \in 6\mathbb{Z}$; thus there exist $k_1, k_2 \in \mathbb{Z}$ such that $x = 4k_1$ and $x = 6k_2$. Now, dividing by $\gcd(6,4) = 2$ we obtain $2k_1 = 3k_2$. Then, since $\gcd(2,3) = 1$, it must be that $2 \mid k_2$. Thus, there exists $k_3 \in \mathbb{Z}$ such that $k_2 = 2k_3$. Then $x = 6k_2 = 6(2k_3) = 12k_3$. Therefore, $x \in 12\mathbb{Z}$, so $4\mathbb{Z} \cap 6\mathbb{Z} \subseteq 12\mathbb{Z}$.

To prove the converse, let x be an arbitrary element in $12\mathbb{Z}$. Thus, for some $k \in \mathbb{Z}$, $x = 12k$. Then it clearly follows that $x = 4(3k)$ and $x = 6(2k)$; therefore $x \in 4\mathbb{Z}$ and $x \in 6\mathbb{Z}$. Thus $x \in 4\mathbb{Z} \cap 6\mathbb{Z}$ as required. ∎

Proof. Let x be an arbitrary element in $m\mathbb{Z} \cap n\mathbb{Z}$. Then $x \in m\mathbb{Z}$ and $x \in n\mathbb{Z}$; thus there exist $k_1, k_2 \in \mathbb{Z}$ such that $x = nk_1$ and $x = mk_2$. Let $d = \gcd(n,m)$. Dividing by d we obtain $\frac{n}{d}k_1 = \frac{m}{d}k_2$. Then, since $\gcd\left(\frac{n}{d}, \frac{m}{d}\right) = 1$, it must be that $\frac{n}{d} \mid k_2$. Thus, there exists $k_3 \in \mathbb{Z}$ such that $k_2 = \frac{n}{d}k_3$. Then $x = mk_2 = m\left(\frac{n}{d}k_3\right) = \frac{mn}{d}k_3$. Now $\frac{mn}{d} = \operatorname{lcm}(m,n) = f$. Thus $x \in f\mathbb{Z}$.

To prove the converse, let x be an arbitrary element in $f\mathbb{Z}$. Thus, for some $k \in \mathbb{Z}$, $x = fk$. Since $f = \operatorname{lcm}(m,n)$, there exist $k_1, k_2 \in \mathbb{Z}$ such that $x = mk_1$ and $x = nk_2$. Therefore, $x \in m\mathbb{Z}$ and $x \in n\mathbb{Z}$. Thus $x \in m\mathbb{Z} \cap n\mathbb{Z}$ as required. ∎

Problem 6

Let S be the set of all polynomials in $\mathbb{Z}[x]$ which have 0 as constant term (that is, polynomials in the form $a_1x + a_2x^2 + \cdots + a_nx^n$.) Show that S is a subring of $\mathbb{Q}[x]$.

Proof. Clearly S is not empty. There is no way for the subtraction of two polynomials in S to produce a non-zero constant term, since both polynomials have constant term 0. There is no way for the multiplication of two polynomials in S to produce a non-zero constant term, since this would require the multiplication of two non-zero constant terms. Thus S is closed under subtraction and multiplication, and by Theorem 7.1, S is a subring of $\mathbb{Q}[x]$. ∎

Problem 7

Let f be some polynomial with rational coefficients, with $deg(f) > 0$, and let S be the set of all polynomials g in $\mathbb{Q}[x]$ for which f divides g. Show that S is a subring of $\mathbb{Q}[x]$. How is this exercise related to the previous exercise?

Proof. Let ϕ, ψ be arbitrary elements in S. Then $f\theta_1 = \phi$ and $f\theta_2 = \psi$ for some $\theta_1, \theta_2 \in \mathbb{Q}[x]$. Then $\phi - \psi = f\theta_1 - f\theta_2 = f(\theta_1 - \theta_2)$. Since $\theta_1 - \theta_2 \in \mathbb{Q}[x]$, it follows that $\phi - \psi \in S$. Thus S is closed under subtraction. Similarly, $\phi\psi = (f\theta_1)(f\theta_2) = f(f\theta_1\theta_2)$. Since $f\theta_1\theta_2 \in \mathbb{Q}[x]$, it follows that $\phi\psi \in S$. Thus S is closed under multiplication. Since $0 = f \cdot 0 \in S$, it follows by Theorem 7.1 that S is a subring of $\mathbb{Q}[x]$. ∎

Solution: The previous problem is a specific case where $f = x$.

Problem 8

(a) Show that the set $\{(a, a) \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$.
(b) Now consider the set $\{(a, -a) \mid a \in \mathbb{Z}\}$. Show that this set is closd under subtraction, but not closed under multiplication, and so is *not* a subring of $\mathbb{Z} \times \mathbb{Z}$.

Proof. Notice $(1, 1) \in \{(a, a) \mid a \in \mathbb{Z}\} \neq \emptyset$. Let $(a, a), (b, b)$ be arbitrary elements in $\{(a, a) \mid a \in \mathbb{Z}\}$. Then $(a, a) - (b, b) = (a - b, a - b) \in \{(a, a) \mid a \in \mathbb{Z}\}$. Thus $\{(a, a) \mid a \in \mathbb{Z}\}$ is closed under subtraction. Similarly, $(a, a)(b, b) = (ab, ab) \in \{(a, a) \mid a \in \mathbb{Z}\}$. Thus $\{(a, a) \mid a \in \mathbb{Z}\}$ is closed under multiplication. It follows by Theorem 7.1 that $\{(a, a) \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$. ∎

Proof. Let $(a, -a), (b, -b)$ be arbitrary elements in $\{(a, -a) \mid a \in \mathbb{Z}\}$. Then $(a, -a) - (b, -b) = (a - b, -a + b) = (a-b, -(a-b)) \in \{(a, -a) \mid a \in \mathbb{Z}\}$. Thus $\{(a, -a) \mid a \in \mathbb{Z}\}$ is closed under subtraction. But $(a, -a)(b, -b) = (ab, -ab)$. Now $ab = -ab$ iff $ab = 0$, so $\{(a, -a) \mid a \in \mathbb{Z}\}$ is not closed under multiplication. ∎

Problem 9

Show that the intersection of any two subrings of a ring is a subring.

Proof. Let R be a ring, and let S_1, S_2 be two subrings of R. Let x, y be arbitrary elements in $S_1 \cap S_2$. Since $x, y \in S_1$, it follows that $x - y \in S_1$. Similarly, $x - y \in S_2$, so $x - y \in S_1 \cap S_2$. Also, since $x, y \in S_1$, it follows that $xy \in S_1$. Similarly, $xy \in S_2$, so $xy \in S_1 \cap S_2$. Finally, note that $0 \in S_1$ and $0 \in S_2$, so $0 \in S_1 \cap S_2$ and the intersection is nonempty. By Theorem 7.1, $S_1 \cap S_2$ is a subring of R. ∎

Problem 10

Show by example that the union of any two subrings of a ring need *not* be a subring. *Hint:* You can certainly find such an example by working in $\mathbb{Z}$.

Solution: Consider $2\mathbb{Z}$ and $3\mathbb{Z}$ which are subrings of $\mathbb{Z}$. Notice, $2 \in 2\mathbb{Z}$ and $3 \in 3\mathbb{Z}$ thus $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, but $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Thus, $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

Problem 16

Suppose that R is a ring with unity, and R has at least two elements. Prove that the additive identity of R is not equal to the multiplicative identity.

Proof. Suppose $1 \in R$ is both the additive and multiplicative identity. Furthermore, let a be an element in R not equal to 1. Then $a+1 = a$ and $a \cdot 1 = a$, thus $a+1 = a \cdot 1 = a$. But this means $a = 0$, and since a was arbitrary, for all $x \in R$, $x = 0$, contradicting that R has more than one element. ∎

Problem 17

Show that if a ring has unity, it is unique.

Proof. Let R be a ring with unity. Suppose $x, y \in R$ are both the unity in R. Then $x \cdot y = x$ and $x \cdot y = y$, thus $x = y$. ∎

Problem 18

(a) Let R be a ring, and consider the set $R \times \mathbb{Z}$ of all ordered pairs with entries from R and $\mathbb{Z}$. Equip this set with operations $(r, n) + (s, m) = (r + s, n + m)$ and $(r, n)(s, m) = (rs + mr + ns, nm)$. Prove that these operations make $R \times \mathbb{Z}$ a ring. (Note that this is *not* the same ring discussed in Example 6.10.)
(b) Show that $R \times \mathbb{Z}$ under these operations has unity, even if R does not.
(c) Show that $R \times \{0\}$ is a subring of the ring $R \times \mathbb{Z}$. Argue that this ring is "essentially the same" as R. (*Note:* Later in the book we will make precise the notion of two rings which are "essentially the same", by defining the *ring isomorphism*.) This means that any ring without unity can essentially be found as a subring of a ring which has unity.

Proof. (**Rule 1**)

$$[(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f) = ((a + c) + e, (b + d) + f).$$

Then the following holds since $R, \mathbb{Z}$ are both rings.

$$((a + c) + e, (b + d) + f) = (a + (c + e), b + (d + f)) = (a, b) + (c + e, d + f) = (a, b) + [(c, d) + (e, f)].$$

(**Rule 2**)

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b),$$

(**Rule 3**)

$$(a, b) + (0_R, 0) = (a + 0_R, b + 0) = (a, b),$$

(**Rule 4**)

$$(a, b) + (-a, -b) = (a - a, b - b) = (0_R, 0),$$

(**Rule 5**)

$$\begin{aligned}[(a,b)(c,d)](e,f) &= (ac+da+bc, bd)(e,f)\\ &= \big((ac+da+bc)e + f(ac+da+bc) + (bd)e,\ (bd)f\big)\\ &= \big(a(ce)+a(de)+b(ce)+a(fc)+a(fd)+b(fc),\ b(df)\big)\\ &= (a,b)(ce+fc+de,\ df)\\ &= (a,b)[(c,d)(e,f)].\end{aligned}$$

(**Rule 6 Left**)

$$\begin{aligned}(a,b)\big[(c,d)+(e,f)\big] &= (a,b)(c+e, d+f)\\ &= \big(a(c+e)+(d+f)a+b(c+e),\ b(d+f)\big)\\ &= (ac+da+bc, bd)+(ae+fa+be, bf)\\ &= (a,b)(c,d)+(a,b)(e,f).\end{aligned}$$

(**Rule 6 Right**)

$$\begin{aligned}\big[(a,b)+(c,d)\big](e,f) &= (a+c, b+d)(e,f)\\ &= \big((a+c)e+f(a+c)+(b+d)e,\ (b+d)f\big)\\ &= (ae+fa+be, bf)+(ce+fc+de, df)\\ &= (a,b)(e,f)+(c,d)(e,f).\end{aligned}$$

∎

Proof. Let $(r,n) \in R \times \mathbb{Z}$. Then

$$\begin{aligned}(r,n)(0_R,1) &= (r\cdot 0_R + 1\cdot r + n\cdot 0_R,\ n\cdot 1) = (r,n),\\ (0_R,1)(r,n) &= (0_R\cdot r + n\cdot 0_R + 1\cdot r,\ 1\cdot n) = (r,n).\end{aligned}$$

∎

Proof. Let R be a ring. Consider the subset $R\times\{0\} = \{(r,0) \mid r \in R\} \subseteq R\times\mathbb{Z}$. Let $(r,0),(s,0)$ be arbitrary elements in $R\times\{0\}$. Since $r,s \in R$, it follows that $(r,0)-(s,0) = (r-s,0) \in R\times\{0\}$. Also, since $r,s \in R$, it follows that $(r,0)(s,0) = (rs+0\cdot r+0\cdot s, 0\cdot 0) = (rs,0) \in R\times\{0\}$. Finally, note that $(0_R,0) \in R\times\{0\}$, so the subset is nonempty. By Theorem 7.1, $R\times\{0\}$ is a subring of $R\times\mathbb{Z}$. The map $r \longrightarrow (r,0)$ preserves addition and multiplication, so $R\times\{0\}$ behaves exactly like R. ∎

8 Integral Domains and Fields

Problem 1

Prove that if R is a commutative ring and $a \in R$ is a zero divisor, then ax is also a zero divisor or 0, for all $x \in R$.

Proof. Suppose R is a commutative ring and $a \in R$ is a zero divisor. Then there exists $b \in R$ with $b \neq 0$ such that $ab = 0$. Now, let x be an arbitrary element of R. If $ax = 0$, then we are done. Suppose $ax \neq 0$. Then $(ax)b = a(xb) = (ab)x = 0$. Since $b \neq 0$, it follows that ax is a zero divisor. ∎

Problem 6

Use Fermat's Little Theorem 8.7 to find $[6]^{-1}$ in $\mathbb{Z}_{19}$.

Proof. In $\mathbb{Z}_{19}$ the theorem asserts that $[6]^{18} = [1]$. But then $[6][6]^{17} = [1]$ so $[6]^{-1} = [6]^{17} = [16]$. ∎

Problem 7

Use Euclid's Algorithm to find $[36]^{-1}$ in $\mathbb{Z}_{101}$.

Proof. First notice $1 = 5 \cdot 101 - 14 \cdot 36$. Thus $-14 \cdot 36 = 1 \pmod{1}01$. Therefor $[36]^{-1} = [-14] = [87]$. ∎

Problem 9

Suppose that $b \in R$, a non-commutative ring with unity. Suppose that $ab = bc = 1$; that is, b has a **right inverse** c and a **left inverse** a. Prove that $a = c$ and that b is a unit.

Proof. Now $a = a \cdot 1 = a(bc) = (ab)c = 1 \cdot c = c$ as required. It directly follows that b is a unit. ∎

Problem 11

Let R be a commutative ring with unity. Suppose that n is the least postivive integer for which we get 0 when we add 1 to itself n times; we then say R has a **characteristic n**. If there exists no such n, we say that R has **characteristic 0**. For example, the characteristic of $\mathbb{Z}_5$ is 5 because $1 + 1 + 1 + 1 + 1 = 0$, whereas $1 + 1 + 1 + 1 \neq 0$. (Note that here we have suppressed '[' and ']'.)
(a) Show that, if the characteristic of a commutative ring with unity R is n and a is *any* of R, then $na = 0$. (Recall that $na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$.)
(b) What are the characteristics of $\mathbb{Q}, \mathbb{R}, \mathbb{Z}_{17}$?
(c) Prove that if a field F has characteristic n, where $n > 0$, then n is a prime integer.

Proof. Notice

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}} = a\underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} = a \cdot 0 = 0.$$

∎

Solution: $\mathbb{Q}$ and $\mathbb{R}$ have characteristic 0. Finally, $\mathbb{Z}_{17}$ has characteristic 17.

Proof. Suppose F is a field with characteristic n where $n > 0$. For contradiction, suppose n is not prime, so $n = ab$ for some a, b with $1 < a, b < n$. Since F is a field, it has no zero divisors, so $0 = n \cdot 1 = (a \cdot 1)(b \cdot 1)$. Now either $a \cdot 1 = 0$ or $b \cdot 1 = 0$ either of which is a contradiction. ∎

Problem 12

Consider the commutative ring $F = \{0, 1, \alpha, 1+\alpha\}$, where 0 is the additive identity, 1 is the mutliplicative identity, $x + x = 0$, for all $x \in F$, and $\alpha^2 = 1 + \alpha$.
(a) Write out explicitly the addition and mutliplication tables for F.
(b) Prove that F is a field.
(c) Because F has four elements, you might expect F would be the "same" as the ring $\mathbb{Z}_4$. Show this is false, by computing the characteristics of F and $\mathbb{Z}_4$ (see the previous exercise).

Solution (a):

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Proof. Notice $1 \cdot 1 = 1$ and

$$\alpha \cdot (1+\alpha) = \alpha + \alpha^2 = \alpha + (\alpha + 1) = 1.$$

Since every nonzero element has a multiplicative inverse, F is a field. ∎

Solution (c): In F, $1+1=0$ but in $\mathbb{Z}_4$, $1+1+1+1=0$ and $1+1 \neq 0$. So they are not the same ring.

Problem 14

Prove that $\mathbb{Z}_m$ is the union of three mutually disjoint subsets: its zero divisors, its units, and $\{0\}$. Show by example that this is false for an arbitrary commutative ring.

Proof. $\{0\}$ is clearly not a zero divisor or a unit in $\mathbb{Z}_m$. Now, suppose $a \in \mathbb{Z}_m$ is a zero divisor and a unit. Then there exists $b \neq 0$ such that $ab = 0$. But then $a^{-1}ab = a^{-1}0 \implies 1 \cdot b = 0 \implies b = 0$, a contradiction.

Now suppose $a \in \mathbb{Z}_m$ and $a \neq 0$. If $\gcd(a,m) = 1$ then a is a unit. Suppose $\gcd(a,m) = d > 1$. Then, there exists $k_1, k_2 \in \mathbb{Z}$ such that $a = dk_1$ and $m = dk_2$. Then $a = dk_1 \iff ak_2 = dk_2k_1 = mk_1 \equiv 0 \pmod{m}$. Thus a is either a unit or a zero divisor.

A counterexample is the trivial ring. ∎

9 Polynomials over a Field

Problem 2

(a) Why does every non-zero complex number have exactly two square roots?
(b) Given part a, check that the proof of the quadratic formula obtained in Exercise 9.1 still holds in $\mathbb{C}[x]$.
(c) Use the quadratic formula to compute the roots of the polynomials $x^2 - (3+2i)x + (1+3i)$ and $x^2 - (1+3i)x + (-2+2i)$.

Solution (a): The book states a non-zero complex number $\alpha = |\alpha|(\cos\theta + i\sin\theta) = |\alpha|e^{i\theta}$ has a square root $\beta = |\alpha|^{1/2}(\cos(\theta/2) + i\sin(\theta/2))$. Any square root of α must have argument $\theta/2 \pmod{\pi}$, so the only square roots are β and $-\beta$.

Solution (b): Checked, and it still holds.

Solution (c): The roots of $x^2-(3+2i)x+(1+3i)$ are $\frac{-(-(3+2i))\pm\sqrt{(-(3+2i))^2-4(1+3i)}}{2}$. The roots of $x^2-(1+3i)x+(-2+2i)$ are $\frac{-(-(1+3i))\pm\sqrt{(-(1+3i))^2-4(-2+2i)}}{2}$.

Problem 3

Give examples of two different polynomials in $\mathbb{Z}_5[x]$ that are identical as functions over $\mathbb{Z}_5$. This shows that equality of polynomials in $F[x]$ cannot be thought of as equality of the corresponding polynomial *functions*. (See the Quick Exercise in Section 4.1 for $F = \mathbb{Z}_2$ case, and Exercise 4.12 for the $F = \mathbb{Z}_3$.)

Solution: By Fermat's little Theorem in $\mathbb{Z}_5$ the polynomials x^5 and x are equivalent for all x.

Problem 4

Consider the polynomial $f = x^3 + 3x^2 + 2x \in \mathbb{Z}_6[x]$. Show that this polynomial has more than three roots in $\mathbb{Z}_6$. Why doesn't this contradict the Root Theorem?

Solution: We can manually check that $x = 0, 1, 2, 3$ are roots. The Root Theorem is about fields and $\mathbb{Z}_6$ is not a field.

Problem 8

Show that if f is a polynomial with real coefficients and $\alpha = s + ti$ is a root of f in $\mathbb{C}$, then so is $\overline{\alpha} = s - ti$.

Proof. Let α, β be complex numbers. We have the following two properties of the algebra of complex numbers

1. $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$.
2. $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$.

Suppose f has real coefficients. Note that for a coefficient $x \in R$, $x = \overline{x}$. From this it clearly follows that $f(\overline{\alpha}) = \overline{f(\alpha)}$. But then suppose $f(\alpha) = 0$ and it follows that $f(\overline{\alpha}) = \overline{f(\alpha)} = \overline{0} = 0$. ∎

Problem 12

In this exercise, we describe the cubic formula for factoring an arbitrary polynomial of degree 3 in $\mathbb{R}[x]$. This version of the formula is called the *Cardano-Tartaglia* formula, after two 16th-century Italian mathematicians involved in its discovery. Consider the polynomial $f = x^3 + ax^2 + bx + c \in \mathbb{R}[x]$ (by dividing by the leading coefficient if necessary, we have assumed without loss of generality that it is 1).

(a) Show that the change in variables $x = y - \frac{1}{3}a$ changes f into a cubic polynomial that lacks a square term; that is, a polynomial of the form $g = f(y - \frac{1}{3}a) = y^3 + py + q = 0$. *Note:* This process is called *depressing the conic*. Clearly we can solve $f = 0$ for x if and only if we can solve $g = 0$ for y.

(b) Find explicit solutions u, v to the pair of simultaneous equations ① $v^3 - u^3 = q$ and ② $uv = \frac{1}{3}p$.

(c) Prove the identity $(u - v)^3 + 3uv(u - v) + (v^3 - u^3) = 0$ and use it to show that $y = u - v$ is a solution to the cubic equation $y^3 + py + q = 0$.

(d) Let $D = q^2 + \frac{3p^3}{27}$. (This is called the *discriminant* of the conic.) Conclude that $y = \sqrt[3]{\frac{-q+\sqrt{D}}{2}} - \sqrt[3]{\frac{q+\sqrt{D}}{2}}$ is a root for $g = 0$. (This is just $u - v$.)

Proof.

$$\begin{aligned} f\Big(y - \frac{1}{3}a\Big) &= \Big(y - \frac{1}{3}a\Big)^3 + a\Big(y - \frac{1}{3}a\Big)^2 + b\Big(y - \frac{1}{3}a\Big) + c \\ &= y^3 + \left(b - \frac{a^2}{3}\right)y + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right). \end{aligned}$$

∎

Proof. If $p = 0$, then $u = v = 0$. Suppose $p \neq 0$. From ② we know $u \neq 0$ and $v \neq 0$. From ②, $v = \frac{p}{3u}$. Plugging this into ① gives

$$\left(\frac{p}{3u}\right)^3 - u^3 = q.$$

Multiplying through by $u^3 \neq 0$ gives

$$\left(\frac{p}{3}\right)^3 - u^6 = u^3 q \quad \iff \quad u^6 + qu^3 - \left(\frac{p}{3}\right)^3 = 0.$$

Letting $x = u^3$ we have the quadratic

$$x^2 + qx - \left(\frac{p}{3}\right)^3 = 0.$$

Applying the quadratic formula gives

$$x = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2}.$$

Taking cube roots shows

$$u = \sqrt[3]{\frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2}}.$$

Finally, from ② we get

$$v = \frac{p}{3\sqrt{\frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2}}}.$$

∎

Proof. Expanding $(u - v)^3 + 3uv(u - v)$, we have

$$\begin{aligned}(u - v)^3 + 3uv(u - v) &= u^3 - 3u^2 v + 3uv^2 - v^3 + 3uv(u - v) \\ &= u^3 - 3u^2 v + 3uv^2 - v^3 + 3u^2 v - 3uv^2 \\ &= u^3 - v^3.\end{aligned}$$

Therefore

$$(u - v)^3 + 3uv(u - v) + (v^3 - u^3) = 0.$$

∎

Proof. Since $uv = \frac{p}{3}$ and $v^3 - u^3 = q$, we have

$$(u - v)^3 + 3uv(u - v) + (v^3 - u^3) = 0.$$

Substituting $3uv = p$ and $v^3 - u^3 = q$ shows

$$(u - v)^3 + p(u - v) + q = 0.$$

∎

Proof. From part b we know

$$u = \sqrt[3]{\frac{-q + \sqrt{D}}{2}}, \quad v = \sqrt[3]{\frac{q + \sqrt{D}}{2}}.$$

Therefore,

$$y = u - v = \sqrt[3]{\frac{-q + \sqrt{D}}{2}} - \sqrt[3]{\frac{q + \sqrt{D}}{2}}$$

is a root of $g(y) = y^3 + py + q = 0$ as required. ∎

Problem 13

In Exercise 12, there is an apparent ambiguity arising from the plus or minus when extracting the square root of D to obtain values for u^3 and v^3. However, show that we obtain the same value value for the root $u - v$, regardless of which choice is made.

Proof. We have the equation $v^3 - u^3 = q$, which any choice of roots satisfies. Viewing our polynomial

$$(u - v)^3 + 3uv(u - v) + (v^3 - u^3) = 0,$$

we showed in Exercise 12 that $(u-v)^3+3uv(u-v) = -(v^3-u^3)$, which is independent of our choice of roots. ∎

Problem 15

Suppose as in Exercise 12 that $g = y^3 + px + q$ is a cubic polynomial with real coefficients, and $y = u - v$ is the root given by the Cardano-Tartaglia formula. Suppose that $D > 0$. (Thus u and v are real numbers.) Let $\zeta = e^{\frac{2\pi}{3}}$ be a cube root of unity (called the primitive cube root of unity in Exercise 25 below). Argue that the other two distinct roots of $g = 0$ are the complex conjugates of $u\zeta - v\zeta^2$ and $u\zeta^2 - v\zeta$. *Note:* be sure and check both that these are roots and that they are necessarily distinct.

Proof. Let $y_1 = u - v, y_2 = \zeta - v\zeta^2, y_3 = u\zeta^2 - v\zeta$. Notice

$$\begin{aligned}(u\zeta - v\zeta^2)^3 + 3uv(u\zeta - v\zeta^2) + (v^3 - u^3) &= u^3\zeta^3 - v^3(\zeta^2)^3 - 3uv(u\zeta - v\zeta^2) + 3uv(u\zeta - v\zeta^2) + (v^3 - u^3)\\ &= u^3 - v^3 - 3uv(u\zeta - v\zeta^2) + 3uv(u\zeta - v\zeta^2) + (v^3 - u^3)\\ &= 0\end{aligned}$$

Similarly,

$$\begin{aligned}(u\zeta^2 - v\zeta)^3 + 3uv(u\zeta^2 - v\zeta) + (v^3 - u^3) &= u^3(\zeta^2)^3 - v^3\zeta^3 - 3uv(u\zeta^2 - v\zeta) + 3uv(u\zeta^2 - v\zeta) + (v^3 - u^3)\\ &= u^3 - v^3 - 3uv(u\zeta^2 - v\zeta) + 3uv(u\zeta^2 - v\zeta) + (v^3 - u^3)\\ &= 0\end{aligned}$$

We show that y_2 and y_3 are complex conjugates:

$$\overline{y_2} = \overline{u\zeta - v\zeta^2} = u\overline{\zeta} - v\overline{\zeta^2} = u\zeta^2 - v\zeta = y_3.$$

Clearly $y_1 \neq y_2$ and $y_1 \neq y_3$ since its imaginary part is 0. Additionally the imaginary parts of y_2 and y_3 are opposite in sign, so $y_2 \neq y_3$. Thus the roots are distinct. ∎

Problem 17

An interesting and suprising conclusion one can draw from example 15 is that if the discriminant of $D > 0$, then the cubic polynomial $y^3 + py + q \in \mathbb{R}[x]$ necessarily has exactly one real root, and a conjugate pair of complex roots. In this exercise you will use elementary calculus to verify this fact again:

1. Consider the function $g(y) = y^3 + py + q$. Suppose that $p > 0$. Compute the derivative of $g'(y)$, and use it to argue that g has exactly one real root, and consequently two complex roots.
2. Suppose now that $p = 0$. Then conclude that $q \neq 0$. In this simple case, what are the roots of g.
3. Now suppose that $p < 0$, Compute the two roots of $g'(y) = 0$. Argue that the values of g at these two roots are both positive (using the assumption that $D > 0$). Why does this mean that g has exactly one root?

Proof. $g'(y) = 3y^2 + p$. Since the deriviative is always > 0 the function is always increasing thus can only cross the real x-axis once. Therefore there is a single real root. ∎

Proof. If $q = 0$ then $D = 0$. The roots are 0. ∎

Proof. Notice

$$3y^2 + p = 0 \quad \Rightarrow \quad y^2 = -\frac{p}{3} \quad \Rightarrow \quad y = \pm\sqrt{-\frac{p}{3}}.$$

Let $y_1 = \sqrt{-p/3}$ and $y_2 = -\sqrt{-p/3}$ be the critical points. Since the discriminant $D > 0$, the values $g(y_1)$ and $g(y_2)$ have the same sign. Thus the cubic can only cross the y-axis once so $g(y)$ as one real root. ∎

Problem 19

Exercise 18 is a particular example of what is called the *irreducible* case for a real cubic. Show that in the case $D < 0$, we obtain real roots for the polynomial $g = y^3 + px + q$ by an appropriate choice of u and v.

Proof. Choose v to be the complex conjugate of u. ∎

Problem 26

A field F is said to be **algebraically closed** if every polynomial $f \in F[x]$ with $deg(F) \geq 1$ has a root in F; we can rephrase this definition roughly by saying that a field is algebraically closed if it satisfies the Fundamental Theorem of Algebra. Thus, $\mathbb{C}$ is algebraically closed, while $\mathbb{R}$ and $\mathbb{Q}$ are not. Show that for every prime p, the field $\mathbb{Z}_p$ is not algebraically closed.

Proof. From Fermat's little theorem $f(x) = x^p - x$ evaluates to 0 for all $x \in \mathbb{Z}_p$. Then $g(x) = f(x) + 1$ evaluates to 1 for all $x \in \mathbb{Z}_p$. Therefore $\mathbb{Z}_p$ is not algebraically closed. ∎

Problem 27

Show that the field in Exercise 8.12 is not algebraically closed. (See the previous exercise for a definition.)

1. The field $F = \{0, 1, \alpha, 1 + \alpha\}$.
2. 0 is the additive idenitty.
3. 1 is the multiplicative identity.
4. $x + x = 0$ for all $x \in F$, and $\alpha^2 = \alpha + 1$.

Proof. Consider $f(x) = x^4 - x$. Then

$$f(0) = 0$$

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

$$f(\alpha) = \alpha^4 - \alpha = (\alpha^2)^2 - \alpha = (\alpha + 1)^2 - \alpha = (\alpha^2 + 1) - \alpha = (\alpha + 1 + 1) - \alpha = \alpha + \alpha = 0$$

$$f(1 + \alpha) = (1 + \alpha)^4 - (1 + \alpha) = ((1 + \alpha)^2)^2 - (1 + \alpha) = (\alpha)^2 - (1 + \alpha) = \alpha^2 - (1 + \alpha) = (\alpha + 1) - (1 + \alpha) = 0$$

Then $g(x) = f(x) + 1 = 1$ for all $x \in F$, thus F is not algebraically closed. ∎

Problem 28

Show that, if F is a field with infinitely many elements, then $f(x) = g(x)$ for all $x \in F$ implies that $f = g$ as polynomials. (We have already seen that this is not the case if F is a finite field. For example, consider $x^2 + x + 1$ and 1 in $\mathbb{Z}_2[x]$.)

Proof. Suppose F is a field with infinitely many elements and $f(x) = g(x)$ for all $x \in F$. Then $\psi(x) = f(x) - g(x) = 0$ for all $x \in F$ and thus has infinitely many roots. But a nonzero polynomial over a field can only have a finite number of roots thus ψ must be the zero polynomial. Therefore $f = g$. ∎

10 Associates and Irreducibles

Problem 1

Find all simultaneous solutions to the Diophantine equations $ac - bd = 1$, $ad + bc = 0$ directly, by eliminating variables, interpret your solutions as determining all units in the Gaussian integers.

Proof. Now, if $c = 0$ then $ad = 0$ implies $a = 0$ or $d = 0$. Suppose $a = 0$ then $-bd = 1$ so $b = 1,\ d = -1$ or $b = -1,\ d = 1$. Suppose $d = 0$ then $ac = 1$ so $a = 1,\ c = 1$ or $a = -1,\ c = -1$.

Now, suppose $c \neq 0$. Then $ad + bc = 0 \iff bc = -ad \iff b = -\frac{ad}{c}$. Plugging in we find

$$ac - \left(-\frac{ad}{c}\right)d = 1 \iff ac + \frac{ad^2}{c} = 1 \iff a(c^2 + d^2) = c \iff a = \frac{c}{c^2 + d^2}.$$

Which only has solutions $c^2 + d^2 = 1$.

Thus the solutions are $a = \pm 1,\ b = 0,\ c = \pm 1,\ d = 0$ or $a = 0,\ b = \pm 1,\ c = 0,\ d = \pm 1$. ∎

Problem 2

Prove Theorem 10.1. That is, let n, be a square-free integer. As in the text, define $N(a+b\sqrt{n}) = |a^2 - nb^2|$. Prove that N preserves multiplication, that is, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. Let $\alpha = a + b\sqrt{n}$ and $\beta = c + d\sqrt{n}$. Then

$$N(\alpha\beta) = N((a + b\sqrt{n})(c + d\sqrt{n})) = N(ac + ad\sqrt{n} + bc\sqrt{n} + bdn)$$

$$= N((ac + bdn) + (ad + bc)\sqrt{n}) = |(ac + bdn)^2 - n(ad + bc)^2|.$$

Similarly

$$N(\alpha)N(\beta) = N(a + b\sqrt{n})N(c + d\sqrt{n}) = |a^2 - nb^2||c^2 - nd^2|.$$

Then

$$(ac + bdn)^2 - n(ad + bc)^2 = a^2c^2 + 2abcd\,n + b^2d^2n^2 - n(a^2d^2 + 2abcd + b^2c^2),$$

which simplifies to

$$a^2c^2 - na^2d^2 - nb^2c^2 + n^2b^2d^2.$$

Then

$$(a^2 - nb^2)(c^2 - nd^2) = a^2c^2 - na^2d^2 - nb^2c^2 + n^2b^2d^2.$$

Thus $N(\alpha\beta) = N(\alpha)N(\beta)$. ∎

Problem 3

Suppose that n, m are distinct square-free integers. Prove that $\mathbb{Z}[\sqrt{n}] \cap \mathbb{Z}[\sqrt{m}] = \mathbb{Z}$. This is not true if at least one of the integers n and m is not square-free. Give an example to show this.

Theorem 4. *Suppose n, m are square free integers such that $n \neq m$ and $a, b \in \mathbb{Z}$. Futhermore, suppose $a \neq 0, b \neq 0$ and $x = a\sqrt{n} - b\sqrt{m}$. Then x is an irrational number.*

Proof. For contradiction, suppose x is rational. Then $x = a\sqrt{n} - b\sqrt{m} \iff x + b\sqrt{m} = a\sqrt{n} \iff \frac{x+b\sqrt{m}}{a} = \sqrt{n}$. Now squaring both sides we find $\frac{x^2+2xb\sqrt{m}+b^2m}{a^2} = n \iff x^2 + 2xb\sqrt{m} + b^2m = a^2n \iff 2xb\sqrt{m} = a^2n - x^2 - b^2m$. Now the rhs is an integer but the lhs is irrational which is a contradiction. ∎

Proof. Let x be an arbitrary element in $\mathbb{Z}[\sqrt{n}] \cap \mathbb{Z}[\sqrt{m}]$. Then $x = a + b\sqrt{n}$ and $x = c + d\sqrt{m}$ for some $a, b, c, d \in \mathbb{Z}$. Then $a + b\sqrt{n} = c + d\sqrt{m} \iff b\sqrt{n} - d\sqrt{m} = c - a$. Now the lhs is irrational unless $b = d = 0$. Thus $a = c$ and $x \in \mathbb{Z}$. Conversely, any integer $z \in \mathbb{Z}$ is in both $\mathbb{Z}[\sqrt{n}]$ and $\mathbb{Z}[\sqrt{m}]$, so $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{n}] \cap \mathbb{Z}[\sqrt{m}]$. Thus, $\mathbb{Z}[\sqrt{n}] \cap \mathbb{Z}[\sqrt{m}] = \mathbb{Z}$. ∎

Proof. Let $n = 2$ and $m = 8$. Then $\sqrt{8} = 2\sqrt{2}$ and thus $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[\sqrt{8}]$. Therefore,

$$\mathbb{Z}[\sqrt{2}] \cap \mathbb{Z}[\sqrt{8}] = \mathbb{Z}[\sqrt{2}] \neq \mathbb{Z}.$$

∎

Problem 4

Prove that the Diophantine equation $2b^2 = a^2 + 3$ has no integer solutions, proceeding similarly as the problem $a^2 = 2b^2 + 3$ is handled in the text in Example 10.16.

Proof. Now $2b^2 = a^2 + 3 \iff a^2 = 2b^2 - 3$, thus a is odd and can be written as $2k_1 + 1$ with $k_1 \in \mathbb{Z}$. Then $(2k_1 + 1)^2 = 2b^2 - 3 \iff 4k_1^2 + 4k_1 + 1 = 2b^2 - 3 \iff 2(2k_1^2 + 2k_1 + 2) = 2b^2$. Thus $b^2 = 2k_1^2 + 2k_1 + 2$, so b is even and can be written as $2k_2$ for some $k_2 \in \mathbb{Z}$. Substituting, we obtain $2(2k_2)^2 = a^2 + 3 \iff 2k_2^2 = k_1^2 + 1$. But this equation has the same form as the original with smaller positive integers. Repeating this process contradicts the well-ordering principle for positive integers, and thus there are no integer solutions. ∎

Problem 5 breakable

Find infinitely many distinct units in $\mathbb{Z}[\sqrt{7}]$. Then list inifintely many associates of $\sqrt{7}$ in $\mathbb{Z}[\sqrt{7}]$.

11 Symmetries of Figures in the Plane

Problem 1

Complete the analysis of the symmetries of the square, which we begin in the text. Some will be rotations, and some will be flips. Determine the matrix and permutation representations for them, draw a table of correspondence, and compute the group table for your symmetries.

Group Table:

$\circ$	ι	p	p^2	p^3	φ	$p\varphi$	φp	φp^2
ι	ι	p	p^2	p^3	φ	$p\varphi$	φp	φp^2
p	p	p^2	p^3	ι	$p\varphi$	φp^2	φ	φp
p^2	p^2	p^3	ι	p	φp	φp^2	$p\varphi$	φ
p^3	p^3	ι	p	p^2	φp^2	φ	φp	$p\varphi$
φ	φ	φp	φp^2	$p\varphi$	ι	p	p^2	p^3
$p\varphi$	$p\varphi$	φp^2	φ	φp	p	p^2	p^3	ι
φp	φp	$p\varphi$	φp^2	φ	p^2	p^3	ι	p
φp^2	φp^2	φ	$p\varphi$	φp	p^3	ι	p	p^2

Permutations:

$$\iota \longleftrightarrow \begin{bmatrix}1&2&3&4\\1&2&3&4\end{bmatrix}, p \longleftrightarrow \begin{bmatrix}1&2&3&4\\4&1&2&3\end{bmatrix}, p^2 \longleftrightarrow \begin{bmatrix}1&2&3&4\\3&4&1&2\end{bmatrix}, p^3 \longleftrightarrow \begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}$$

$$\varphi \longleftrightarrow \begin{bmatrix}1&2&3&4\\2&1&4&3\end{bmatrix}, p\varphi \longleftrightarrow \begin{bmatrix}1&2&3&4\\3&2&1&4\end{bmatrix}, \varphi p \longleftrightarrow \begin{bmatrix}1&2&3&4\\1&4&3&2\end{bmatrix}, \varphi p^2 \longleftrightarrow \begin{bmatrix}1&2&3&4\\4&3&2&1\end{bmatrix}$$

Table of Correspondence:

	1	2	3	4
ι	1	2	3	4
p	4	1	2	3
p^2	3	4	1	2
p^3	2	3	4	1
φ	2	1	4	3
$p\varphi$	3	2	1	4
φp	1	4	3	2
φp^2	4	3	2	1

Matrix Correspondence:

$$\iota \longleftrightarrow \begin{bmatrix}1&0\\0&1\end{bmatrix}, p \longleftrightarrow \begin{bmatrix}0&-1\\1&0\end{bmatrix}, p^2 \longleftrightarrow \begin{bmatrix}-1&0\\0&-1\end{bmatrix}, p^3 \longleftrightarrow \begin{bmatrix}0&1\\-1&0\end{bmatrix}$$

$$\varphi \longleftrightarrow \begin{bmatrix}1&0\\0&-1\end{bmatrix}, p\varphi \longleftrightarrow \begin{bmatrix}0&1\\1&0\end{bmatrix}, \varphi p \longleftrightarrow \begin{bmatrix}0&-1\\-1&0\end{bmatrix}, \varphi p^2 \longleftrightarrow \begin{bmatrix}-1&0\\0&1\end{bmatrix}$$

Problem 3

Determine all symmetries of a non-square rectangle, and represent them with matrices and permutations. How many rotations, and how many are flips.

Proof. We simply remove the square symmetries constructed from 1 or 3 rotations. Thus there are 4 symmetries of a non-square rectangle. ∎

Problem 5

Show algebraically that the rotation transformation preserves distance: Consider the points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$.
(a) What is the square of the distance between P_1 and P_2.
(b) Now rotate through the angle θ, by multiplying by the appropriate matrix, to obtain the points $P_1'(x_1', y_1')$ and $P_2'(x_2', y_2')$. Compute the square of the distance of these points. Use trig identities to show that this is the same as in part a.

Solution (a): The square of the distance between P_1 and P_2 is $(x_2 - x_1)^2 + (y_2 - y_1)^2$.

Solution (b): Notice

$$\begin{bmatrix} x_1 & y_1 \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} x_1\cos\theta + y_1\sin\theta, & -x_1\sin\theta + y_1\cos\theta \end{bmatrix}$$

$$\begin{bmatrix} x_2 & y_2 \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} x_2\cos\theta + y_2\sin\theta, & -x_2\sin\theta + y_2\cos\theta \end{bmatrix}$$

Thus

$$P_1'(x_1', y_1') = P_1'(x_1\cos\theta + y_1\sin\theta, -x_1\sin\theta + y_1\cos\theta),$$

and

$$P_2'(x_2', y_2') = P_2'(x_2\cos\theta + y_2\sin\theta, -x_2\sin\theta + y_2\cos\theta).$$

Then the square of the distance between these points is

$$((x_2\cos\theta + y_2\sin\theta) - (x_1\cos\theta + y_1\sin\theta))^2 + ((-x_2\sin\theta + y_2\cos\theta) - (-x_1\sin\theta + y_1\cos\theta))^2.$$

Some basic algebra show this simplifies to $(x_2 - x_1)^2 + (y_2 - y_1)^2$.

Problem 6

Verify by mutliplying two matrices together that a rotation through angle θ, followed by a rotation through angle φ, gives a rotation through angle $\theta + \varphi$.

Solution:

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix} = \begin{bmatrix} \cos\theta\cos\phi + (-\sin\theta)(\sin\phi) & \cos\theta(-\sin\phi) + (-\sin\theta)\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & \sin\theta(-\sin\phi) + \cos\theta\cos\phi \end{bmatrix}$$

$$= \begin{bmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi & -\cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & -\sin\theta\sin\phi + \cos\theta\cos\phi \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{bmatrix}$$

Problem 7

How many symmetries can you find for the unit circle? Which rotations are possible? Which flips?

Solution: There are an infinite number of symmetries for both flips and rotations on the unit circle.

Problem 8

Find out how many elements there are in D_n, the group of symmetries of a regular n-sided polygon.

Solution: There are n rotations including the identity. For each of these rotations we can flip granting another n symmetries. Thus there are $2n$ total symmetries.

Problem 9

You can check that all of the matrices of the symmetries of the equilateral triangle and the square have the property that their determinants are always ± 1 (See Exercise 8.2 for a definition of the determinant of a 2×2 matrix.) In this exercise you will show thaSt if a matrix preserves distance, then its determinant must be 1.

(a) Suppose that $A \in M_2(\mathbb{R})$, and let $det(A) = 0$. Show that mutliplication by A cannot preserve distance. Do this by showing that multiplication by A takes some point in the plane to the origin and hence cannot preserve distance.
(b) Suppose next that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = A \in M_2(\mathbb{R}),$$

but $det(A) \neq 0$. Suppose that multiplication by A does preserve distance, and consider successively what happens to

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} d \\ -c \end{bmatrix}, \begin{bmatrix} -b \\ a \end{bmatrix}$$

You will be able to infer that $det(A) = \pm 1$.

Proof. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an arbitrary matrix in $M_2(\mathbb{R})$ such that $\det(A) = 0$. Then $\det(A) = ad - bc = 0$, so $ad = bc$. Let $\begin{bmatrix} x & y \end{bmatrix}$ be a point with $x, y \in \mathbb{R}$. Applying the transformation A gives

$$\begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ax + by & cx + dy \end{bmatrix}.$$

If $a = b = c = d = 0$, then all points are mapped to the origin. Suppose w.l.o.g. that $a \neq 0$. From $ax + by = 0$, we get $x = -\frac{b}{a}y$. Substituting into $cx + dy = 0$ gives

$$c\left(-\frac{b}{a}y\right) + dy = \left(d - \frac{bc}{a}\right) y = 0.$$

Since $\det(A) = ad - bc = 0$, we have $d - \frac{bc}{a} = 0$. Thus, any point on the line $x = -\frac{b}{a}y$ is mapped to the origin by A. ∎

$$A\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}, \quad A\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix},$$

From this it follows that $a^2 + c^2 = 1$ and $b^2 + d^2 = 1$.

$$A\begin{bmatrix} d \\ -c \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d \\ -c \end{bmatrix} = \begin{bmatrix} ad - bc \\ cd - cd \end{bmatrix} = \begin{bmatrix} ad - bc \\ 0 \end{bmatrix}, \quad A\begin{bmatrix} -b \\ a \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} -b \\ a \end{bmatrix} = \begin{bmatrix} -ab + ab \\ -bc + ad \end{bmatrix} = \begin{bmatrix} 0 \\ ad - bc \end{bmatrix}.$$

We see that $|det(A)| = |ad - bc| = 1$ if distance is to be preserved.

Problem 10

Our description of the symmetries of the equilateral triangle can be elegantly rephrased using the arithmetic of the complex numbers $\mathbb{C}$, described in Chapter 8.
(a) Argue that the three vertices of the triangle can be thought of as numbers of the form $e^{i\alpha_i}$ in the complex plane, for appropriate angles α_i.
(b) Show that you can represent the rotations of the triangle in the symmetry group by complex mutliplication by a number of the form $e^{i\theta}$, for an appropriate choice of θ.
(c) What operation on the complex numbers performs the flip ϕ?

Solution (a): The three vertices can be represented as

$$e^{i\alpha_1}, \quad e^{i\alpha_2}, \quad e^{i\alpha_3},$$

where $\alpha_1 = 0$, $\alpha_2 = 2\pi/3$, and $\alpha_3 = 4\pi/3$. The modulus is 1 because the vertices are on the unit circle.

Solution (b): Rotations of the triangle correspond to multiplication by

$$e^{i\theta}, \quad \theta \in \{0, 2\pi/3, 4\pi/3\}.$$

Solution (c): A flip across a line through the origin is represented by complex conjugation $e^{-i\alpha_i}$, possibly combined with multiplication by $e^{i\phi}$.

12 Figures in Space

Problem 1

Find all symmetries of a pyramid as draw below (the base is a square, and the four sides are congruent).

Solution: There are 4 symmetries by rotating the base 3 times plus the identity.

Problem 3

Consider the *flatlanders*, who live in the plane and consequently cannot conceive of motion in three dimensions. Formulate a definition for $\mathbb{R}^2$ for flatlanders, and then determine for them the group of symmetries of the equilateral triangle and the square.

Solution: A symmetry is a one-to-one onto function $\beta : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ which preserves distances and does not reverse the direction of any basis vector. There are 4 symmetries of the square and 3 symmetries of the equilateral triangle under this definition of symmetry in $\mathbb{R}^2$.

Problem 8

Consider a cube with a special down face: This face is different, and consequently, a symmetry must leave it alone; the face might be rotated, but must remain the down face. (You might imagine a circular dot in the center of this face.) How many symmetries of the unmarked cube are still symmetries of this cube.

Solution: The four symmetries that rotate the base.

13 Abstract Groups

Problem 5

In this problem we consider permutations of the set $\mathbb{R}$.
(a) Let $S(\mathbb{R})$ denote the set of all real-valued functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, such that f is *one-to-one* and *onto*. Prove that $S(\mathbb{R})$ is a group, where the operation is functional composition.
(b) Now let $A(\mathbb{R})$ be the set of functions from $S(\mathbb{R})$ that are also **order preserving**: By this we mean that if $x < y$, then $f(x) < f(y)$. Prove that $A(\mathbb{R})$ is a group under functional composition.

Proof. Let $f, g, h \in S(\mathbb{R})$. Furthermore, let $\iota : \mathbb{R} \longrightarrow \mathbb{R}$ be a function defined by $\iota(x) = x$. Notice that $\iota \in S(\mathbb{R})$.

Proof. Let $f, g \in A(\mathbb{R})$. We know that f and g are bijections and order preserving. Let $\iota : \mathbb{R} \to \mathbb{R}$ be defined by $\iota(x) = x$.

(**Rule 1**) Let $x, y \in \mathbb{R}$ such that $x < y$. Since g is order preserving, $g(x) < g(y)$. Since f is order preserving, $f(g(x)) < f(g(y))$. Thus $(f \circ g)(x) < (f \circ g)(y)$. It follows that $f \circ g \in A(\mathbb{R})$.

(**Rule 2**) Suppose $x < y$. Then $\iota(x) < \iota(y)$, so ι is order preserving. Thus $\iota \in A(\mathbb{R})$.

(**Rule 3**) Let $f \in A(\mathbb{R})$. Since f is a bijection, it has an inverse f^{-1}. Let $x, y \in \mathbb{R}$ such that $x < y$. Then $f(x) < f(y)$, and applying f^{-1} gives $f^{-1}(x) < f^{-1}(y)$. It follows that f^{-1} is order preserving, and $f^{-1} \in A(\mathbb{R})$. ∎

(**Rule 1**) Let x be an arbitrary real number. Notice $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$.

(**Rule 2**) Notice that $f \circ \iota = \iota \circ f = f$.

(**Rule 3**) Since f is a bijection, it has an inverse f^{-1} such that $f \circ f^{-1} = f^{-1} \circ f = \iota$. ∎

Problem 7

Let n be a positive integer and $\mathscr{C}$ be a circle. Now for $i = 0, 1, \ldots, n-1$, let p_i be the rotation of $\mathscr{C}$ counterclockwise through the angle $2\pi i/n$ radians. Show that this set of rotations is a group under the operation of composition. How many elements are in this group?

Proof. Let $i, j \in \{x \in \mathbb{Z} \mid 0 \leq x \leq n-1\}$.

(**Rule 1**) Notice that

$$p_i \circ p_j = p_{(i+j) \bmod n} = p_j \circ p_i.$$

It follow that the set of closed under composition.

(**Rule 2**) Notice that

$$p_i \circ p_{(n-i) \bmod n} = p_0.$$

(**Rule 3**) Since p_0 is rotation by angle 0, it follows that

$$p_i \circ p_0 = p_0 \circ p_i = p_i.$$

∎

Solution: There are n elements in this group.

Problem 8

Let G be a group with operation $\circ$. Suppose that $x \circ x = 1$, for all $x \in G$. Prove that G is abelian.

Proof. Let $x, y \in G$. Then $x \circ y = (x \circ y)^{-1} = y^{-1} \circ x^{-1} = y \circ x$ as required. ∎

Problem 10

Let R be any ring, and suppose that $\phi, \psi \in Aut(R)$. Show that the composition of $\phi\psi \in Aut(R)$, by checking that this function has the appropriate domain and range, is one-to-one, onto, and preserves addition and mutiplication. (This exercise verfies that $Aut(R)$ is closed under functional composition; in Example 24.18 we complete the verification that $Aut(R)$ is a group under this operation.)

Proof. Since $dom(\phi\psi) = dom(\psi) = R$, the domain of $\phi\psi$ is valid. Now, since $ran(\psi) = R$ and ϕ is one-to-one and onto, the range of the composition $\phi\psi$ is R.

Let $x, y \in R$. Then $\phi(\psi(x)) = \phi(\psi(y))$, and since ϕ is one-to-one, it follows that $\psi(x) = \psi(y)$. Then, since ψ is one-to-one, $x = y$; thus $\phi\psi$ is one-to-one.

Now let x be an arbitrary element in R. Since ϕ is onto, there exists $y \in R$ such that $\phi(y) = x$. Since $y \in R$ and ψ is onto, there exists $z \in R$ such that $\psi(z) = y$. Then $\phi\psi(z) = x$; thus $\phi\psi$ is onto.

Therefore $\phi\psi : R \longrightarrow R$ is a one-to-one, onto function as required.

Now let x, y be arbitrary elements in R. Then $(\phi\psi)(x+y) = \phi(\psi(x+y)) = \phi(\psi(x)+\psi(y))$. Similarly, $(\phi\psi)(xy) = \phi(\psi(x)\psi(y))$. Thus $\phi\psi$ is closed under addition and multiplication. ∎

Problem 11

Prove that $Aut(\mathbb{Z})$ is a group with only a single element.

Proof. Since $\mathbb{Z}$ is a ring, by problem 10, $\langle Aut(\mathbb{Z}), \circ \rangle$ is a group. Now clearly $\iota \in Aut(\mathbb{Z})$. Let ψ be an arbitrary automorphism in $Aut(\mathbb{Z})$. Consider $\psi(1 \cdot 1) = \psi(1^2) = \psi(1)\psi(1)$. Thus $\psi(1)^2 = \psi(1)$, which in $\mathbb{Z}$ has two solutions: 0 and 1. Suppose $\psi(1) = 0$. Then ψ would map all integers to 0, contradicting bijectivity. To see this, let x be an arbitrary integer. Then $x = \underbrace{1 + 1 + \cdots + 1}_{x \text{ times}}$, and it follows that $\psi(x) = \underbrace{\psi(1) + \psi(1) + \cdots + \psi(1)}_{x \text{ times}} = \underbrace{0 + 0 + \cdots + 0}_{x \text{ times}} = 0$. It follows that $\psi(1) = 1$. Therefore $\psi(x) = x$ for all $x \in \mathbb{Z}$, so $\psi = \iota$. ∎

Problem 11

Show that $Aut(\mathbb{Q})$ is a group with only a single element.

Proof. Since $\mathbb{Q}$ is a ring, by problem 10, $\langle Aut(\mathbb{Q}), \circ \rangle$ is a group. Now clearly $\iota \in Aut(\mathbb{Q})$. Let ψ be an arbitrary automorphism in $Aut(\mathbb{Q})$. Consider $\mathbb{Z} \subset \mathbb{Q}$. By problem 10, we know that for $a \in \mathbb{Z}$, $\psi(a) = a$. Now let $b \in \mathbb{Q} - \{0\}$ and note that $\psi(1) = \psi\left(b \cdot \frac{1}{b}\right) = \psi(b)\psi\left(\frac{1}{b}\right) = b \cdot x = 1$. It must be that $x = \frac{1}{b}$, thus $\psi\left(\frac{1}{b}\right) = \frac{1}{b}$. Then let $x \in \mathbb{Q}$ be written as $\frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{Z} - \{0\}$. It follows that $\frac{a}{b} = a \cdot \frac{1}{b}$ and $\psi\left(a \cdot \frac{1}{b}\right) = \psi(a)\psi\left(\frac{1}{b}\right) = a \cdot \frac{1}{b} = \frac{a}{b}$. Thus $\psi = \iota$, as required. ∎

Problem 13

In this problem you will sketch the proof that $Aut(\mathbb{R})$ is a group with only a single element. You will use the fact that all positive real numbers have exactly two square roots.
(a) Let $a, b, \in \mathbb{R}$. Show that $a \geq b$ if and only if $a - b = x^2$, for some $x \in \mathbb{R}$.
(b) Use part a to show that if $\rho \in Aut(\mathbb{R})$, then $a \geq b$ if and only if $\rho(a) \geq \rho(b)$.
(c) Argue that any automorphism of $\mathbb{R}$ is fixed on the rational numbers $\mathbb{Q}$ (See Exercise 12.)
(d) You may assume that between any two real numbers is a rational number. Use this to prove that any automorphism of $\mathbb{R}$ is fixed on all real numbers, so $Aut(\mathbb{R})$ has only a single element.

Proof. ($\longrightarrow$) Suppose $a \geq b$. It follows that $a - b \geq 0$. Thus since $a - b \in \mathbb{R}$, there exists $x \in \mathbb{R}$ such that $x^2 = a - b$.

($\longleftarrow$) Suppose $a - b = x^2$, for some $x \in \mathbb{R}$. It follows that $x^2 \geq 0$ thus $a \geq b$. ∎

Proof. ($\longrightarrow$) Suppose $\rho \in Aut(\mathbb{R})$. Furthermore, suppose $a \geq b$. Then $a + (-b) = x^2 \geq 0$. Thus $\rho(a + (-b)) = \rho(a) + \rho(-b) = \rho(x^2) \geq \rho(0) = 0$. Therefore $\rho(a) \geq \rho(b)$ as required.

($\longleftarrow$) Suppose $\rho(a) \geq \rho(b)$. Then $\rho(a) - \rho(b) \geq \rho(0) \iff \rho(a + (-b)) \geq \rho(0)$. Thus $a + (-b) \geq 0$ and it follows that $a \geq b$. ∎

Proof. This follows directly from Problem 12 since $\mathbb{Q} \subset \mathbb{R}$. ∎

Proof. Now, since the rationals are fixed, if ρ is not the identity it must be that an irrational number was mapped to a different irrational number. That is, for some $x \in \mathbb{R}$ such that x is irrational, $\rho(x) = z$ such that z is irrational and $x \neq z$. Consider some arbitrary rational number between x and z, say l. Now there are two cases: either $x < l < z$ or $x > l > z$. Then, wlog suppose $x < l < z$. It follows that $\rho(x) < \rho(l) < \rho(z)$, but $\rho(l) = l$ and $\rho(x) = z$, thus $z < l < \rho(z)$, which is a contradiction. Thus the real numbers are fixed. It follows that $Aut(\mathbb{R})$ contains one element ι. ∎

Problem 14

Consider the field of complex numbers $\mathbb{C}$, and its group of automorphisms $Aut(\mathbb{C})$. Show that this group has only two elements, namely the identity automorphism ι, and the complex conjugate map ϕ defined by $\phi(a + b) = a - bi$. (See Exercise 16.4).

Proof. Clearly $\iota \in Aut(\mathbb{C})$. Let $\rho \in Aut(\mathbb{C})$. Then ρ must fix all real numbers from Problem 13. Now consider $\rho(i)$. Since $i^2 = -1$ it follows that $\rho(i)^2 = \rho(i^2) = \rho(-1) = -1$. Thus $\rho(i) = i$ or $\rho(i) = -i$. Therefore, for any $a + bi \in \mathbb{C}$, either $\rho(a + bi) = a + bi$ or $\rho(a + bi) = a - bi$. Thus $Aut(\mathbb{C})$ has exactly two elements: ι and ϕ. ∎

14 Subgroups

Problem 1

Consider the set

$$i\mathbb{R} = \{a_i \mid a \in \mathbb{R}\} \subseteq \mathbb{C}$$

these are the **imaginary** numbers. Prove that this is a subgroup of the additive group $\mathbb{C}$. Is I a subring of the ring $\mathbb{C}$? Similarly, show that $i\mathbb{Z} = \{ni \mid n \in \mathbb{Z}\}$ is a subgroup of the additive group of the Gaussian integers $\mathbb{Z}[i]$.

Proof. Clearly the set is nonempty. Let $xi, yi \in i\mathbb{R}$. Then $xi - yi = (x - y)i \in i\mathbb{R}$. By Theorem 35.2, $i\mathbb{R}$ is a subgroup of $\mathbb{C}$. ∎

Solution: No, $i\mathbb{R}$ is not a subring of $\mathbb{C}$ since it is not closed under multiplication.

Proof. Clearly the set is nonempty. Let $xi, yi \in i\mathbb{Z}$. Then $xi - yi = (x - y)i \in i\mathbb{Z}$. By Theorem 35.2, $i\mathbb{Z}$ is a subgroup of $\mathbb{Z}[i]$. ∎

Problem 2

Prove Theorem 25.1c. That is, suppose that G is a group and $g, h \in G$. Prove that $gx = h$ has a unique solution; likewise, prove that $xg = h$ has a unique solution. (We have written the equations multiplicatively.)

Proof. Notice $gx = h \iff g^{-1}gx = g^{-1}h \iff x = g^{-1}h$. Similarly $xg = h \iff xgg^{-1} = hg^{-1} \iff x = hg^{-1}$. ∎

Problem 3

Prove Theorem 25.1d. That is, prove that in a group, every element has exactly one inverse.

Proof. Suppose G is a group and let $x \in G$. Futhermore, suppose x has two inverses namely: x_1^{-1}, x_2^{-1}. Then $xx_1^{-1} = 1 = xx_2^{-1}$. Then by the cancellation property $x_1^{-1} = x_2^{-1}$. ∎

Problem 4

Prove the subgroup Theorem 25.2: A non-empty subset H of a group G is a subgroup if and only if whenever $h, k \in H$, then $hk^{-1} \in H$.

Proof. Suppose H is a nonempty subset of a group G.

($\longrightarrow$) Suppose H is a subgroup of G. Let h, k be arbitrary elements in H. Since H is a subgroup, $k^{-1} \in H$. Also, since H is closed under multiplication, $hk^{-1} \in H$ as required.

($\longleftarrow$) Suppose that if $h, k \in H$, then $hk^{-1} \in H$.

(**Rule 1**) Associativity holds in G, thus it holds in H.

(**Rule 2**) Since H is nonempty, let $h \in H$. Then $hh^{-1} = 1 \in H$. Thus the multiplicative identity belongs to H.

(**Rule 3**) Let $h \in H$. Since $1, h \in H$, it follows that $1h^{-1} = h^{-1} \in H$. ∎

Problem 5

Show that if H and K are subgroups of the group G, then $H \cap K$ is also a subgroup of G. Show by example that $H \cup K$ need not be a subgroup. (This exercise and should be compared to Exercises 7.9 and 7.10.)

Proof. Suppose H and K are subroups of the group G. Now, $1 \in H$ and $1 \in K$ since they are subgroups thus $1 \in H \cap K$. Therefore, $H \cap K$ is nonempty. Let $x, y \in H \cap K$. We know $xy^{-1} \in H$ and $xy^{-1} \in K$ since H, K are subgroups of G. Thus $xy^{-1} \in H \cap K$. By Theorem 35.2, $H \cap K$ is a subgroup of G. ∎

Proof. Consider the group $\langle \mathbb{Z}, + \rangle$. Let $H = 2\mathbb{Z}$ and $K = 3\mathbb{Z}$. Then H and K are subgroups of $\mathbb{Z}$.

But $2 \in H$ and $3 \in K$, and $2 + 3 = 5 \notin H \cup K$. Thus $H \cup K$ is not closed under addition and therefore is not a subgroup. ∎

Problem 6

Suppose that G is a group, written multiplicatively. Let $g \in G$, and suppose that $g^2 = g$. Prove that g is the identity.

Proof. We have $g^2 = gg = g = g1$. Cancellation on the left shows $g = 1$, as required. ∎

Problem 7

Let G be a group, and $a, b, c \in G$. Prove that the equation $axc = b$ has a unique solution in G.

Proof. Notice $axc = b \iff axcc^{-1} = bc^{-1} \iff ax = bc^{-1} \iff a^{-1}ax = a^{-1}bc^{-1} \iff x = a^{-1}bc^{-1}$. ∎

Problem 8

① Suppose that G is equipped with an associative operation $*$. ② Suppose that G has an element e so that $g * e = g$, for all $g \in G$; ③ futhermore, for all $g \in G$, there exists an element $g' \in G$, so that $g * g' = e$. Why are these assumptions apparently weaker than decreeing that G be a group? Prove, however, that these assumptions are sufficient to force G to be a group.

Solution: A group requires the Rule 2 and 3 to commute.

Proof. (**Rule 1**) It is given that $*$ is associative.

(**Rule 2**) Notice $g * g' = e \iff g * (g' * e) = e② \iff (g * g') * e = e① \iff g * g' = e③$.

(**Rule 3**) ∎

Problem 9

Show that if $(xy)^{-1} = x^{-1}y^{-1}$ for all x and y in the group G. Then G is abelian.

Problem 10

Complete the following multiplicaiton table so tthe following will be a group.

	a	b	c	d
a				
b				d
c			d	
d				

Problem 12

Show that $n\mathbb{Z}$ is a subgroup of the additive group of integers $\mathbb{Z}$, for all integers n.

Proof. Clearly $n\mathbb{Z}$ is nonempty (consider $5n \in \mathbb{Z}$). Let x, y be arbitrary elements in $n\mathbb{Z}$. Thus $x = k_1 n$ and $y = k_2 n$ for some $k_1, k_2 \in \mathbb{Z}$. Then $x - y = k_1 n - k_2 n = (k_1 - k_2)n \in n\mathbb{Z}$. Thus $n\mathbb{Z}$ is closed under subtraction. It follows from Theorem 35.2 that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. ∎

Problem 13

Find all finite subgroups of the additive group $\mathbb{C}$. What can you say about all finite subgroups of the multiplicative group $\mathbb{C}^*$?

Solution: Both have no nontrivial finite subgroups.

Problem 14

Argue *geometrically* that the dihedral group, D_n, has a subgroup of order n.

Problem 15

Let G be a group and $a \in G$. Define the **centralizer** of a to be

$$C(a) = \{g \in G \mid ga = ag\}$$

That is, $C(a)$ consists of all elements that commute with a.
(a) Find $C(\rho)$ in D_3.
(b) Find $C(4)$ in $\mathbb{Z}_7$.
(c) Show that $C(a)$ is a subgroup of G.
(d) Let H be a subgroup of G, and let

$$C(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$$

call $C(H)$ the **centralizer** of H. Show that $C(H)$ is a subgroup of G.

Problem 16

Let $Z(G)$, the **center of** G, be thset of elements of G that commute with all elements of G.
(a) Find the center of the quaternions, defined in Example 24.15.
(b) Find the center of $\mathbb{Z}_5$.
(c) Show that $Z(G)$ is a subgroup of G.
(d) If $Z(G) = G$, what can you say about the group G.

Problem 17

If H is a subgroup of G, then show that $Z(G) \cap H$ is a subgroup of $Z(H)$.

Problem 23

Generalize the situtation in the previous two exercises, replacing 2 and 3 by some positive integer m.