Abstract Algebra done Concretely

Donu Arapura

February 19, 2004

Introduction: I wrote these notes for my math 453 class since I couldn't find a book that covered basic abstract algebra with the level and emphasis that I wanted. Rather than spending a lot of time on axiomatics and serious theorem proving, I wanted to spend more time with examples, simple applications and with making scenic detours. I may have gotten a bit carried away with the detours, and certainly there is more here than can be covered in a semester at a reasonable pace. However, a lot of these side topics (which I marked with a star) can be skipped to save time. In order to try to encourage students to play around with examples, I tried to include some Maple code now and then. But its role is secondary and it can be ignored without losing too much. Also since I wanted to emphasize the mathematics rather than the algorithms, I didn't go out of my way to implement these things efficiently.

If you find typos or more serious errors, send me email.

- Donu Arapura (dvb@math.purdue.edu)

Contents

Chapter 1

Natural Numbers

We want to start with the basic rules, or axioms, of arithmetic in the set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$. This will form a model for much of what we will later.

We can add natural numbers, and this operation satisfies:
The **commutative law**

$$n + m = m + n, \tag{1.1}$$

the **associative law**

$$m + (n + r) = (m + n) + r, \tag{1.2}$$

the **identity property for** 0

$$0 + n = n, \tag{1.3}$$

and the **cancellation law**

$$\text{if } m + n = m + r \text{ then } n = r \tag{1.4}$$

We can now define $m \leq n$, or equivalently $n \geq m$, to mean that the equation

$$n = m + r$$

has a solution $r \in \mathbb{N}$. The solution r is unique by the cancellation law, and we can define $n - m = r$.

Lemma 1.1. *The relation $\leq$ satisfies*

1. *The reflexive property: $n \leq n$.*
2. *The transitive property: if $n \leq m$ and $m \leq r$ then $n \leq r$.*

Proof. The equation $n = 0 + n$ implies that $n \leq n$. Suppose that $n \leq m$ and $m \leq r$, then the equations

$$m = n + a$$

and

$$r = m + b$$

have solutions $a, b \in \mathbb{N}$. Therefore

$$r = m + b = (n + a) + b = n + (a + b)$$

which implies $n \leq r$. $\square$

We impose a few more rules about $\leq$ which don't follow from the definition:
Antisymmetry:

$$m \leq n \text{ and } n \leq m \text{ implies } m = n \tag{1.5}$$

Linear ordering:

$$\text{For any pair } m, n \in \mathbb{N},\ m \leq n \text{ or } n \leq m. \tag{1.6}$$

Well ordering:

$$\text{Any nonempty subset of } \mathbb{N} \text{ has a least element} \tag{1.7}$$

It is this last property which makes the natural numbers special. Often in proofs or in the construction of algorithms, one has a situation where one constructs a decreasing sequence of natural numbers $x_1 > x_2 > \ldots$. The well ordering property implies that this sequence will eventually stop. We can use well ordering to *prove* the principle of mathematical induction.

Theorem 1.2. *Let $P \subseteq \mathbb{N}$ be a subset.*

1. *If $0 \in P$ and $n + 1 \in P$ whenever $n \in P$, then $P = \mathbb{N}$.*
2. *If $0 \in P$ and $n \in P$ whenever $0, 1, \ldots n - 1 \in P$ then $P = \mathbb{N}$.*

In practice, this means that to prove a statement for all natural numbers, say

$$0 + 1 + 2 \ldots n = \frac{n(n+1)}{2},$$

it's enough to check it for 0 (the initial step) and then check that the statement holds for $n + 1$ if it holds for n (the induction step). The second part gives a form of induction that's less familiar but also useful. To see this in action, let's prove the above equation using this form. It certainly holds when $n = 0$. Suppose that we know the equation

$$0 + 1 + 2 \ldots m = \frac{m(m+1)}{2}$$

holds for all natural numbers $m = 0, 1, \ldots n - 1$. Take $m = n - 1$ above, after adding n to both sides and simplifying, we establish the equation for hold for $m = n$. Therefore it holds for all n.

Before giving the proof, we make a few observations. 1 can be *defined* to be the least element of the set of nonzero natural numbers. (If we wanted to be fussy, we should really impose the nonemptiness of this set as a rule.) Therefore $n \neq 0$ implies that $n \geq 1$, from which it follows that $n = m + 1$ for some $m \in \mathbb{N}$.

Proof. 1) Suppose that $P \neq \mathbb{N}$, then the complement $F = \mathbb{N} - P = \{x \in \mathbb{N} \mid x \notin P\}$. is nonempty. Let $n \in F$ be the smallest element. Then $n \neq 0$ since $0 \in P$. Therefore $n = m + 1$. Since $m < n$ it follows that $m \in P$. This implies that $m \in P$. By assumption, $m + 1$ would have to lie in P. But this would be a contradiction.

2) We choose F and $n \in F$ as above. Since n is minimal, it follows that $0, 1, \ldots n - 1 \in P$. Therefore $n \in P$ which is again a contradiction. $\square$

In a more systematic development of natural numbers, we would define multiplication in terms of the more basic operations. The idea is that

$$nx = x + x + \ldots x \text{ (n times)}$$

To avoid confusion, let us denote the right hand side by $mult_x(n)$. We reformulate this as an inductive, or recursive, definition:

$$mult_x(n) = \begin{cases} 0 \text{ if } n = 0 \\ mult_x(n-1) + x \text{ otherwise} \end{cases} \tag{1.8}$$

This makes sense because of the following:

Proposition 1.3. *Given a set A, an element $a \in A$, and a function $g : \mathbb{N} \times A \to A$, there exists a unique function $f : \mathbb{N} \to A$ satisfying*

$$f(n) = \begin{cases} a \textit{ if } n = 0 \\ g(n-1, f(n-1)) \textit{ otherwise} \end{cases}$$

One can make even more elaborate recursive definitions, where $f(n)$ is specified for some initial values of n, and then a formula for general $f(n)$ depending on earlier values. Such a recursive definition is theoretically useful for establishing properties of the function. It also has practical value, in that it leads to a method for computing the function. Namely, one systematically calculates $f(0), f(1), \ldots$. At each stage the required information for calculating $f(n)$ has already been given.

For example the Fibonacci numbers are given by the sequence

$$1, 1, 2, 3, 5, 8 \ldots$$

The pattern is that each number in the sequence is the sum of the previous two. So the nth Fibonacci number is given by

$$fib(n) = \begin{cases} 1 \text{ if } n = 0 \text{ or } n = 1 \\ fib(n-2) + fib(n-1) \text{ otherwise} \end{cases}$$

1.4 Exercises

1. Let $mult_m(n)$ be defined as in (1.8). Prove that $mult_{m+1}(n) = mult_m(n) + n$ by induction on n (treating m as constant).

2. With the help of the previous problem, prove that $mult_m(n) = mult_n(m)$ by induction on n (treating m as constant). This is the commutative law for multiplication: $nm = mn$.

   For the following problems assume all the standard rules of highschool algebra.

3. Let
$$F(n) = \frac{1}{\sqrt{5}}[r^{n+1} - s^{n+1}]$$
   where
$$r = \frac{1+\sqrt{5}}{2},\ s = \frac{1-\sqrt{5}}{2}$$
   (a) Calculate $fib(n)$ and $F(n)$ by hand for $n = 0, 1, 2$, and check that $fib(n) = F(n)$ for these values.

   (b) Repeat above for $n = 3, 4, 5$ using Maple, appendix B.

4. Prove that $fib(n) = F(n)$ for all $n \in \mathbb{N}$.

Chapter 2

Principles of Counting

Natural numbers are important because they can be used to count. Given a natural number $n \in \mathbb{N}$, let

$$[n] = \{x \in \mathbb{N} \mid x < n\} = \{0, 1, 2, \ldots n-1\}$$

Let X be a set, then we say that X has n elements, or that $|X| = n$ if there exists a one to one correspondence $f : [n] \to X$ (see appendix A for definitions of these concepts). If no such n exists, then we say that X is an infinite set. The first problem is to show that $|X|$ cannot have multiple values. This is guaranteed by the following:

Theorem 2.1. *If there exists a one to one correspondence $f : [n] \to [m]$, then $n = m$.*

Proof. We will prove this by induction on the minimum M of n and m. Suppose that M is zero. Then $n = 0$ or $m = 0$. If $n = 0$, then $[n] = \emptyset$, so that $f : \emptyset \to [m]$ is onto. It follows that $m = 0$. If $m = 0$, then $f^{-1} : \emptyset \to [n]$ is onto, so that $n = 0$.

Assume that $M > 0$ and that the theorem holds for $M - 1$. Then define $g : [n-1] \to [m-1]$ by

$$g(i) = \begin{cases} f(i) & \text{if } f(i) < f(n-1) \\ f(i) - 1 & \text{if } f(i) > f(n-1) \end{cases}$$

This is a one to one correspondence, therefore $m - 1 = n - 1$, which implies $m = n$. □

Lemma 2.2. *If a finite set X can be written as a union of two disjoint subsets $Y \cup Z$ (disjoint means their intersection is empty), then $|X| = |Y| + |Z|$.*

Proof. Let $f : [n] \to Y$ and $g : [m] \to Z$ be one to one correspondences. Define $h : [n+m] \to X$ by

$$h(i) = \begin{cases} f(i) & \text{if } i < n \\ g(i-n) & \text{if } i \geq n \end{cases}$$

This is a one to one correspondence. □

A *partition* of X is a decomposition of X as a union of subsets $X = Y_1 \cup Y_2 \cup \ldots Y_n$ such that Y_i and Y_j are disjoint whenever $i \neq j$.

Corollary 2.3. *If $X = Y_1 \cup Y_2 \cup \ldots Y_n$ is a partition, then $|X| = |Y_1| + |Y_2| + \ldots |Y_n|$.*

Corollary 2.4. *If $f : X \to Y$ is a function, then*

$$|X| = \sum_{y \in Y} |f^{-1}(y)|$$

Proof. The collection $\{f^{-1}(y)\}$ forms a partition of X. □

Next consider the cartesian product of two finite sets appendix A.

Theorem 2.5. *If X and Y are finite sets, then $|X \times Y| = |X||Y|$.*

Proof. Let $p : X \times Y \to Y$ be the projection map defined by $p(x, y) = y$. Then

$$p^{-1}(y) = \{(x, y) \mid x \in X\}$$

and $(x, y) \to x$ gives a one to one correspondence to X. Therefore, by the previous corollary,

$$|X \times Y| = \sum_{y \in Y} |p^{-1}(y)| = |Y||X|$$

□

We want to outline a second proof. For this proof, we assume that $X = [m]$ and $Y = [n]$ for some $m, n \in \mathbb{N}$. Then we have to construct a one to one correspondence between $[m] \times [n]$ and $[mn]$. We define a map $L(q, r) = qn + r$ from $[m] \times [n] \to \mathbb{N}$. Since $q \leq m - 1$ and $r \leq n - 1$, we have

$$L(q, r) < (m - 1)n + n = mn$$

So we can regard F is a map from $[m] \times [n] \to [mn]$ which can visualized using the table

L	0	1	...	n-1
0	0	1	...	n-1
1	n	n+1	...	2n-1
⋮	...			
m-1	(m-1)n	...		mn-1

The fact that L is a one to one correspondence is proved by the next theorem which is usually called the "division algorithm". Although it's not an algorithm in the technical sense, it is the basis of the algorithm for long division that one learns in school.

Theorem 2.6. *Let $a, n \in \mathbb{N}$ with $n \neq 0$, then there exists a unique pair of natural numbers q, r satisfying*

$$a = qn + r,\ r < n$$

Furthermore if $a < mn$, then $q < m$.

r is called the remainder of division of a by n.

Proof. Let

$$R = \{a - q'n \mid q' \in \mathbb{N} \text{ and } q'n \leq a\}$$

Let $r = a - qn$ be the smallest element of R. Suppose $r \geq n$. Then $a = qn + r = (q+1)n + (r-n)$ means that $r - n$ lies in R. This is a contradiction, therefore $r < n$.

Suppose that $a = q'n + r'$ with $r' < n$. Then $r' \in R$ so $r' \geq r$. Then $qn = q'n + (r' - r)$ implies that $n(q - q') = r' - r$. So $r' - r$ is divisible by n. On the other hand $0 \leq r' - r < n$. But 0 is the only integer in this range divisible by n is 0. Therefore $r = r'$ and $qn = q'n$ which implies $q = q'$.

For the last part, suppose that $a < mn$. If $q \geq m$, then $a \geq qn \geq mn$ which is a contradiction. □

Since the r and q above are unique (given a and n), we can view them as functions $r(a, n)$ and $q(a, n)$. In Maple, these functions are denoted by $irem(a, n)$ and $iquo(a, n)$ respectively.

2.7 Exercises

1. Suppose that $m = n = 101$. What's $L^{-1}(5234)$?
2. Given finite sets Y, Z. Prove that $|Y \cup Z| = |Y| + |Z| - |Y \cap Z|$.
3. If $B \subseteq A$, prove that $|A - B| = |A| - |B|$. Use this to prove that the set of distinct pairs $\{(x_1, x_2) \in X \times X \mid x_1 \neq x_2\}$ has $|X|^2 - |X|$ elements.
4. Suppose that a dice is rolled twice.
   a) In how many ways can a five or six be obtained on the first role?
   b) In how many ways can a five or six be obtained in either (or both) roll(s)?
   c) In how many ways can the same number be rolled twice?
   d) In how many ways can different numbers be obtained for each roll?
5. Prove corollary 2.3 by induction.

Chapter 3

Integers and Abelian groups

The set integers $\mathbb{Z} = \{\ldots -2, -1, 0, 1, \ldots\}$ is obtained by adding negative numbers to the set of natural numbers. This makes arithmetic easier.

Addition satisfies the rules (1.1), (1.2), (1.3) as before. In addition, there is new operation $n \mapsto -n$ satisfying

$$\text{For each } n \in \mathbb{Z},\ n + (-n) = 0 \tag{3.1}$$

The cancellation law becomes redundant as we will see.

We will now abstract this:

Definition 3.1. *An Abelian group consists of a set A with an associative commutative binary operation $*$ and an identity element $e \in A$ satisfying $a * e = a$ and such that any element a has an inverse a' which satisfies $a * a' = e$.*

Abelian groups are everywhere. Here list a few some examples.

Let $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0\}$ be the set of rational numbers, the $\mathbb{R}$ the set of real numbers and $\mathbb{C}$ the set of complex numbers.

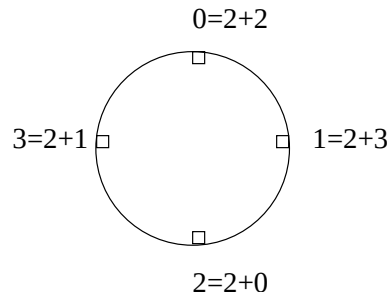
Example 3.2. *The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ with $* = +$ and $e = 0$ are Abelian groups.*

Example 3.3. *The set $\mathbb{Q}^*$, (or $\mathbb{R}^*$ or $\mathbb{C}^*$) of nonzero rational (or real or complex) numbers with $* = \cdot$ (multiplication) and $e = 1$ is an Abelian group. The inverse in this case is just the reciprocal.*

Example 3.4. *Let n be a positive integer. Let $\mathbb{Z}^n = \{(a_1, a_2, \ldots a_n) | a_1, \ldots a_n \in \mathbb{Z}\}$. We define $(a_1, \ldots a_n) + (b_1, \ldots b_n) = (a_1 + b_1, \ldots a_n + b_n)$ and $\mathbf{0} = (0, \ldots 0)$. Then $\mathbb{Z}^n$ becomes an Abelian group. $\mathbb{Z}$ can be replaced by $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ and these examples are probably familiar from linear algebra.*

Example 3.5. *Let n be a positive integer, $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$. Arrange these on the face of a "clock". We define a new kind of operation $\oplus$ called addition $\bmod n$. To compute $a \oplus b$, we set the "time" to a and then count off b hours. We'll give a more precise description later. Unlike the previous examples, this is a finite Abelian group.*

Often, especially in later sections, we will simply use $+$ instead $\oplus$ because it easier to write. We do this in the diagram below:



Here's the addition table for $\mathbb{Z}_8$.

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Notice that the table is symmetric (i.e. interchanging rows with columns gives the same thing). This is because the commutative law holds. The fact that that 0 is the identity corresponds to the fact that the row corresponding 0 is identical to the top row. There is one more notable feature of this table: every row contains each of the elements $0, \ldots 7$ exactly once. A table of elements with this property is called a *latin square*. As we will see this is always true for any Abelian group.

We can now define the precise addition law for $\mathbb{Z}_n$. Given $a, b \in \mathbb{Z}_n$, $a \oplus b = r(a+b, n)$, where r is the remainder introduced before.

When doing calculations in Maple, we can use the mod operator. For example, to add $32 \oplus 12$ in $\mathbb{Z}_{41}$, we just type

$$32 + 12 \, mod \, 41;$$

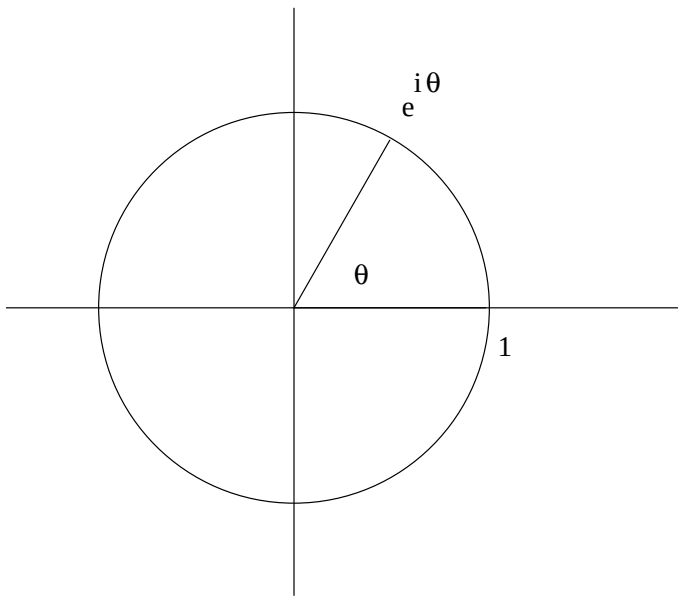
Let n be a positive integer, a complex number z is called an nth root of unity if $z^n = 1$. Let μ_n be the set of all nth roots of unity. For example, $\mu_2 = \{1, -1\}$ and $\mu_4 = \{1, -1, i, -i\}$.

Example 3.6. *μ_n becomes an Abelian group under multiplication*

To see that this statement make sense, note that given two elements $z_1, z_2 \in \mu_n$, their product lies in μ_n since $(z_1 z_2)^n = z_1^n z_2^n = 1$ and $1/z_1 \in \mu_n$ since

$(1/z_1)^n = 1$. We can describe all the elements of μ_n with the help of Euler's formula:

$$e^{i\theta} = \cos\theta + i\sin\theta.$$



Lemma 3.7. $\mu_n = \{e^{i\theta} \mid \theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots \frac{2(n-1)\pi}{n}\}$

Proof. The equation $z^n = 1$ can have at most n solutions since it has degree n (we will prove this later on). So it's enough to verify that all of the elements on the right are really solutions. Each element is of the form $z = e^{i\theta}$ with $\theta = 2\pi k/n$ with k an integer. Then

$$z^n = e^{in\theta} = \cos(2\pi k) + i\sin(2\pi k) = 1.$$

□

The lemmas says that the elements are equally spaced around the unit circle of $\mathbb{C}$.

Since $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$, multiplication amounts to adding the angles. This sounds suspiciously like the previous example. We will see they are essentially the same.

Lemma 3.8. *(Cancellation) Suppose that $(A, *, e)$ is an Abelian group. Then $a * b = a * c$ implies $b = c$.*

Proof. By assumption, there exists a' with $a' * a = a * a' = e$. Therefore

$$a' * (a * b) = a' * (a * c)$$

$$(a' * a) * b = (a' * a) * c$$

$$e * b = e * c$$
$$b = c.$$

□

Corollary 3.9. *Given a, there is a unique element a', called the inverse, such that $a * a' = e$.*

Lemma 3.10. *The multiplication table*

$*$	a_1	$\dots$
a_1	$\dots$	
$\vdots$		

of any Abelian group $A = \{a_1, a_2, \dots\}$ forms a symmetric latin square.

Proof. The symmetry follows from the commutative law. Suppose that $A = \{a_1, a_2, \dots\}$. Then the ith row of the table consists of $a_i * a_1, a_i * a_2 \dots$. Given $a \in A$, the equation $a = a_i * (a_i' * a)$ shows that a occurs somewhere in this row. Suppose that it occurs twice, that is $a_i * a_j = a_i * a_k = a$ for $a_j \neq a_k$. Then this would contradict the cancellation lemma. □

Let $(A, *, e)$ be a group. Given $a \in A$ and $n \in \mathbb{Z}$, define a^n by

$$a^n = \begin{cases} a * a \dots a \text{ (} n \text{ times) if } n > 0 \\ e \text{ if } n = 0 \\ a' * a' \dots a' \text{(} -n \text{ times) if } n < 0 \end{cases}$$

Often the operation on A is written as $+$, in which case the inverse of a is usually written as $-a$, and we write na instead of a^n. When $A = \mathbb{Z}$, this nothing but the definition of multiplication. It's possible to prove the associative, commutative and distributive laws for $\mathbb{Z}$, but we'll skip this.

3.11 Exercises

1. Let $A = \{e, a, b\}$ with e, a, b distinct and the following multiplication table:

*	e	a	b
e	e	a	b
a	a	e	b
b	b	b	a

   Is A an Abelian group? Prove it, or explain what goes wrong.

2. Let $A = \{e, a\}$ with $a \neq e$ and the following multiplication table:

*	e	a
e	e	a
a	a	e

Is A an Abelian group? Prove it, or explain what goes wrong.

3. Let $(A, *, e)$ be an Abelian group. Let a' denote the inverse of a. Prove that $e' = e$, $(a')' = a$ and $(a * b)' = a' * b'$.

4. With notation as above, prove that $(a^n)' = (a')^n$ for any natural number n by induction. This proves $(a^n)^{-1} = (a^{-1})^n = a^{-n}$ as one would hope.

5. Let $(A, *, e)$ and $(B, *, \epsilon)$ be two Abelian groups. Let $A \times B = \{(a, b) \mid a \in A, b \in B\}$. Define $(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$ and $E = (e, \epsilon)$. Prove that $(A \times B, *, E)$ is an Abelian group. This is called the direct product of A and B. For example $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$.

6. Write down the multiplication tables for μ_2, μ_3, μ_4 and μ_5.

7. An element $\omega \in \mu_n$ is called a primitive root if any element can be written as a power of ω. Check that $e^{2\pi i/5} \in \mu_5$ is primitive. Determine all the others in this group.

Chapter 4

Divisibility

Given two integers a and b, we say a divides b or that b is a multiple of a or $a|b$ if there exists an integer q with $b = aq$. Some basic properties divisibility are given in the exercises. It is a much subtler relation than $\leq$. A natural number p is called *prime* if $p \geq 2$ and if the only natural numbers dividing are 1 and p itself.

Lemma 4.1. *Every natural number $n \geq 2$ is divisible by a prime.*

Proof. Let $D = \{m \mid m|n \text{ and } m \geq 2\}$. D is nonempty since it contains n. Let p be the smallest element of D. If p is not prime, there exists $d|p$ with $2 \leq d < p$. Then $d \in D$ by exercise 1 of this chapter, but this contradicts the minimality of p. □

Corollary 4.2. *(Euclid) There are infinitely many primes.*

Proof. Suppose that are only finite many primes, say $p_1, p_2, \ldots p_n$. Then consider $N = p_1 p_2 \ldots p_n + 1$. Then N must be divisible by a prime which would have to be one of the primes on the list. Suppose it's p_k. Then by exercise 2, $1 = N - p_1 p_2 \ldots p_n$ would be divisible by p_k, but this is impossible. □

The following is half of the fundamental theorem of arithmetic. What's missing is the uniqueness statement and this will be proved later.

Corollary 4.3. *Every natural number $n \geq 2$ is a product of primes.*

The statement will be proved by induction on n. Note that we have to start the induction at $n = 2$. This does not entail any new principles, since we can change variables to $m = n - 2$, and do induction on $m \geq 0$.

Proof. $n = 2$ is certainly prime. By induction, we assume that the statement holds for any $2 \leq n' < n$. By the lemma, $n = pn'$ with p prime and n' a natural number. If $n = p$ then we are done. Otherwise $n' \geq 2$, so that it can be written as a product of primes. Therefore the same goes for $n = pn'$. □

The proofs can be turned into a method, or algorithm, for factoring an integer. In fact, it's the obvious one. Start with n, try to divide by $2, 3, 4 \ldots n-1$. If none of these work, then n is prime. Otherwise, record the first number, say p, which divides it; it's a prime factor. Replace n by n/p and repeat. Similarly, we get an algorithm for testing whether n is prime, by repeatly testing divisibility by $2, 3, 4 \ldots n-1$. Note that we can do slightly better (ex. 3)

4.4 Exercises

1. Prove that $|$ is transitive, and that $a|b$ implies that $a \leq b$ provided that $b > 0$.

2. Prove that $a|b$ and $a|c$ implies $a|(b'b + c'c)$ for any pair of integers b', c'.

3. Prove that in the above primality algorithm, it's enough to test divisibility by integers $2, 3, 5, 7 \ldots k$ where k is the biggest odd number $\leq \sqrt{n}$.

Let $b \geq 2$ be an integer. A base b expansion of a natural number N is a sum $N = a_n b^n + a_{n-1} b^{n-1} + \ldots a_0$ where each a_i is an integer satisfying $0 \leq a_i < b$. Base 10 (decimal) expansions are what we normally use, but $b = 2, 8, 16$ are useful in computer science.

4 Show that a_0 is the remainder of division of N by b.

5 For any $b \geq 2$, prove that any natural number N has a base b expansion by induction. (Use the division algorithm.)

6 Turn the proof around to find a method for calculating the coefficients a_i. Find a base 8 expansion of 1234.

7 The proof of corollary 4.2 suggests the following strategy for generating primes: multiply the first n consecutive primes and add 1. For example, $2 + 1, (2)(3) + 1$ and $(2)(3)(5) + 1$ are all prime. Does this always work? You can, and probably should, use a computer for this. The $isprime(x)$ procedure in Maple can be used to test if x prime[1].

8 Modify the proof of corollary 4.2 to prove that for any prime p, there exists a prime $p < q \leq p! + 1$.

[1] Actually it uses a probabilistic test which could fail for really huge values of x. But that won't be a problem here.

Chapter 5

Congruences

Fix a positive integer n. For doing computations in $\mathbb{Z}_n$ with paper and pencil, it's very convenient to introduce the $\equiv$ symbol. We will say that $a \equiv_n b$ if $a - b$ is divisible by n, or equivalently if a and b. One can work with $\equiv$ symbol as one would for $=$ thanks to:

Proposition 5.1. *The follow hold:*

1. $\equiv_n$ *is reflexive, i.e.* $x \equiv_n x$.
2. $\equiv_n$ *is symmetric, i.e.* $x \equiv_n y$ *implies* $y \equiv_n x$.
3. $\equiv_n$ *is transitive, i.e.* $x \equiv_n y$ *and* $y \equiv_n z$ *implies that* $x \equiv_n z$.
4. *If* $a \equiv_n b$ *and* $c \equiv_n d$ *then* $a + c \equiv_n b + d$.

Proof. We prove the transitivity (3). The other statements are left as an exercise. Suppose that $x \equiv_n y$ and $y \equiv_n x$, then $x - y = na$ and $y - z = nb$ for some $a, b \in \mathbb{Z}$. Then $x - z = x - y + y - z = n(a + b)$, which proves that $x \equiv_n z$. $\square$

A relation satisfying the first three properties above is called an *equivalence relation*.

Lemma 5.2. *Given an integer* x *and a positive integer* n*, there exist a unique element* $(x \, mod \, n) \in \{0, 1, \ldots n - 1\}$ *such that* $x \equiv_n (x \, mod \, n)$

A warning about notation. Our use of *mod* as an operator is consistent with the way it's used in Maple but it's not the way it's used in most math books. Typically, they would write $x \equiv y \, (\, mod \, n)$ instead of $x \equiv_n y$.

Proof. First suppose $x \geq 0$. In this case, there are no surprises. The division algorithm gives $x = qn + r$ with $r \in \{0, \ldots n - 1\}$. $x \equiv_n r$ since n divides $x - r$. So we can take $x \, mod \, n = r$.

Suppose that $x < 0$. If x is divisible by n, then we take $x \, mod \, n = 0$. Suppose is x is not divisible by n, then applying the division algorithm to $-x$ yields $-x = qn + r$ with $0 < r < n$. Therefore

$$x = -qn - r = -qn - n + n - r = -(q+1)n + (n - r)$$

with $0 < n - r < n$. So we can take $x \, mod \, n = n - r$. We leave it as an exercise to check the uniqueness. $\square$

The proof shows that $x \, mod \, n$ is just the remainder $r(x, n)$ when $x \geq 0$. When $x < 0$, there doesn't seem to be any clear consensus on what the remainder should be, some people think it should be $x \, mod \, n$ and others think it should be the negative number $-r(-x, n)$ (Maple's *irem* follows the latter convention).

$x \to x \, mod \, n$ can be visualized as follows when $n = 3$

$$\begin{array}{ccccccc} -3 & -2 & -1 & 0 & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 \end{array}$$

The rule for adding in $\mathbb{Z}_n$ is now quite easy with this notation. Given $x, y \in \{0, 1, \ldots n-1\}$

$$x \oplus y = (x + y) \, mod \, n$$

Now we can finally prove:

Theorem 5.3. $(\mathbb{Z}_n, +, 0)$ *is an Abelian group.*

Proof. We assume that the variables $x, y, z \in \{0, 1, \ldots n-1\}$. Let's start with the easy properities first.

$$x \oplus y = (x + y) \, mod \, n = (y + x) \, mod \, n = y \oplus x$$

$$x \oplus 0 = (x + 0) \, mod \, n = x$$

Set

$$\ominus x = (-x) \, mod \, n$$

Then, either $x = 0$ in which case

$$x \oplus (\ominus x) = 0 + 0 \, mod \, n = 0,$$

or else $x \neq 0$ in which case $\ominus x = n - x$ so that

$$x \oplus (\ominus x) = (x + n - x) \, mod \, n = 0.$$

Finally, we have to prove the associative law. We have

$$y + z \equiv_n (y + z \, mod \, n) = y \oplus z$$

by definition. Therefore by proposition 5.1

$$x + (y + z) \equiv_n x + (y \oplus z) \equiv_n (x + (y + z \, mod \, n)) \, mod \, n = x \oplus (y \oplus z)$$

On the other hand

$$x + y \equiv_n (x + y \, mod \, n) = x \oplus y$$

so that

$$(x + y) + z \equiv_n (x \oplus y) + z \equiv_n ((x \oplus y) + z) \, mod \, n = (x \oplus y) \oplus z$$

Since $x + (y + z) = (x + y) + z$, we can combine these congruences to obtain

$$x \oplus (y \oplus z) \equiv_n (x \oplus y) \oplus z$$

We can conclude that the two numbers are the same by the uniquess statement of lemma 5.2.

□

5.4 Exercises

1 Given that September 4, 2002 is a Wednesday, calculate the day of the week of September 4, 2012 using arithmetic in $\mathbb{Z}_7$. Note that 2004, 2008, 2012 are leap years.

2 Finish the proof of proposition 5.1.

3 Prove the uniqueness part of lemma 5.2, i.e. suppose that $y, z \in \{0, 1, \ldots n-1\}$ both satisfy $x \equiv_n y$ and $x \equiv_n z$, prove that $y = z$.

4 Prove that if $a \equiv_n b$ and $c \equiv_n d$ then $ac \equiv_n bd$.

5 Let $\theta = 2\pi/n$. Prove that if x and y are integers such that $x \equiv_n y$, then $e^{ix\theta} = e^{iy\theta}$.

Chapter 6

Linear Diophantine equations

Given two integers a, b, a common divisor is an integer d such that $d|a$ and $d|b$. The greatest common divisor is exactly that, the common divisor greater than or equal to all others (it exists since the set of common divisors is finite). We denote this by $gcd(a, b)$.

Lemma 6.1 (Euclid). *If a, b are natural numbers then $gcd(a, b) = gcd(b, a \bmod b))$*

Proof. Let $r = a \bmod b$. Then the division algorithm gives $a = qb + r$ for some q. It follows from exercise 2 of the chapter 4 that $gcd(b, r)|a$. Since $gcd(b, r)|b$, we can conclude that $gcd(b, r) \leq gcd(a, b)$. On the other hand, $r = a - qb$ implies that $gcd(a, b)|r$. Therefore $gcd(a, b)$ is a common divisor of b and r, so $gcd(a, b) \leq gcd(b, r)$. $\square$

This lemma leads to a method for computing gcds. For example

$$gcd(100, 40) = gcd(40, 20) = gcd(20, 0) = 20.$$

A *Diophantine equation* is an equation where the solutions are required to be integers or rationals. The simplest examples are the linear ones: given integers a, b, c, find all integers m, n such that $am + bn = c$. If a solution exists, then $gcd(a, b)$ must divide c by exercise 2 of chapter 4. The converse is also true:

Theorem 6.2. *Given integers a, b, c, $am + bn = c$ has a solution with $m, n \in \mathbb{Z}$ if and only if $gcd(a, b)|c$.*

Proof. Since $(m', n') = (\pm m, \pm n)$ is a solution of $\pm an' + \pm bm' = c$, we may as well assume that $a, b \geq 0$. We now prove the theorem for natural numbers a, b by induction on the minimum $min(a, b)$.

If $min(a, b) = 0$, then one of them, say $b = 0$. Since $a = gcd(a, b)$ divides c by assumption, $(c/a, 0)$ gives a solution of $am + bn = c$. Now assume that $a'm + b'n = c'$ has a solution whenever $min(a', b') < min(a, b)$ and the other

conditions are fulfilled. Suppose $b \leq a$, and let $r = r(a,b) = a \, mod \, b$ and $q = q(a,b)$ be given as in theorem 2.6. Then $rm' + bn' = c$ has a solution since $min(r,b) = r < b = min(a,b)$ and $gcd(b,r) = gcd(a,b)$ divides c. Let $m = n'$ and $n = m' - qn'$, then

$$am + bn = an' + b(m' - qn') = bm' + rn' = c.$$

□

Corollary 6.3. *Given $a, b \in \mathbb{Z}$, there exists $m, n \in \mathbb{Z}$ such that $am + bn = gcd(a,b)$.*

The proof yields a method for finding a solution. For simplicity assume that $a \geq b \geq 0$. Then a solution to $am + bn = c$ is given by $m = s_1(a,b,c), n = s_2(a,b,c)$ where these functions are given recursively:

$$\begin{aligned} s_1(a,b,c) &= \begin{cases} c/a \text{ if b=0} \\ s_2(b, r(a,b), c) \text{ otherwise} \end{cases} \\ s_2(a,b,c) &= \begin{cases} 0 \text{ if b=0} \\ s_1(b, r(a,b), c) - q(a,b) s_2(b, r(a,b), c) \text{ otherwise} \end{cases} \end{aligned}$$

This is easy to implement in Maple:

```
 s1 := (a,b,c) -> if (b=0) then
                    c/a
                   else
                    s2(b,irem(a,b),c)
                   fi;
s2 := (a,b,c) -> if (b=0) then
                     0
                  else
                     s1(b, irem(a,b),c)-iquo(a,b)*s2(b,irem(a,b),c)
                  fi;
```

Lemma 6.4. *If p is prime number, then for any integers, $p|ab$ implies that $p|a$ or $p|b$.*

Proof. Suppose that p does not divide a, then we have to show that it divides b. By assumption, we can write $ab = cp$ for some integer c. Since p is prime, and $gcd(p,a)|p$, $gcd(p,a)$ is either 1 or p. It must be 1, since $gcd = p$ would contradict the first statement. Therefore $pm + an = 1$ for some integers m, n. Multiply this by b to obtain $p(bm + cn) = b$. So $p|b$. □

Corollary 6.5. *Suppose that $p|a_1 \ldots a_n$, then $p|a_i$ for some i.*

The proof of the corollary is left as an exercise.

We can now finish the proof of the fundamental theorem of arithmetic.

Theorem 6.6. *A natural number $N \geq 2$ can be expressed as a product of primes in exactly one way. What that means if $N = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ where $p_1 \leq p_2 \leq \dots p_n$ and $q_1 \leq \dots q_m$ are primes, then $n = m$ and $p_i = q_i$.*

Proof. The existence part has already been done in corollary 4.3. We will prove that given increasing finite sequences of primes such that

$$p_1 \dots p_n = q_1 \dots q_m, \tag{6.1}$$

then $m = n$ and $p_i = q_i$ by induction on the minimum $min(n, m)$. We will interpret the initial case $min(m, n) = 0$ to mean that 1 is not a product of primes, and this is clear. Now suppose that (6.1) holds, and that $0 < n \leq m$. Then p_1 divides the right side, therefore p_1 divides some q_i. Since q_i is prime, $p_1 = q_i$. Similarly $q_1 = p_j$ for some j. We can conclude that $p_1 = q_1$, since $q_1 \leq q_i$ and $q_i = p_1 \leq p_j \leq q_1$. Canceling p_1 from (6.1) leads to an equation $p_2 \dots p_n = q_2 \dots q_m$. By induction, we are done. □

6.7 Exercises

1. Carry out the procedure explained after lemma 6.1 to calculate $gcd(882, 756)$. (Do this by hand.)

2. Prove that any common divisor of a and b divides $gcd(a, b)$, and conversely that any divisor of the gcd is a common divisor.

3. The least common multiple $lcm(a, b)$ of two natural numbers a, b is the smallest element of the set of numbers divisible by both a and b. Prove that $lcm(a, b) = \frac{ab}{gcd(a,b)}$.

4. Given integers a, b, determine all integer solutions to $am + bn = 0$. Assuming the existence of one solution (m_0, n_0) to $am + bn = c$, determine all the others.

5. In how many ways, can you express \$10 as a sum of dimes and quarters? (This is a linear diophantine equation with an obvious constraint.)

6. Find one solution for $120m + 131n = 1$ (either by hand or using Maple).

7. Prove corollary 6.5.

Chapter 7

Subgroups of Abelian groups

Let's return to the subject of Abelian groups. We introduce a way of producing new examples from old.

Definition 7.1. *A subset B of an Abelian group $(A, *, e)$ is a subgroup if*

1. $e \in B$
2. *B is closed under $*$: $a, b \in B \Rightarrow a * b \in B$.*
3. *B is closed under inversion: if $a \in B$ then the inverse $a' \in B$.*

In fact, you've something like this before in your linear algebra classes. This is similar to the notion of subspace.

Lemma 7.2. *A subgroup of an Abelian group is again an Abelian group.*

Example 7.3. *$\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, and this is a subgroup of $\mathbb{R}$, and this is a subgroup $\mathbb{C}$.*

Example 7.4. *The set of even numbers is a subgroup of $\mathbb{Z}$. More generally, for any integer n, the set of multiples of n, denoted by $n\mathbb{Z}$ is a subgroup. The verification is straight forward. $0 = n0 \in \mathbb{Z}$. If a, b are integers then $na + nb = n(a + b)$ and $-na = n(-a)$, so $n\mathbb{Z}$ is closed under addition and inverses.*

Example 7.5. *μ_n is a subgroup of $\mathbb{C}^*$. In fact, we checked all the conditions in the discussion following example 3.6.*

Let $\mathbb{Z}^n$ denote the Abelian group of integer vectors

$$\mathbb{Z}^n = \{(m_1, \dots m_n) \mid m_i \in \mathbb{Z}\}$$

with addition given by

$$(m_1, \dots m_n) + (m_1', \dots m_n') = (m_1 + m_1', \dots m_n + m_n')$$

and identity

$$0 = (0, \dots 0).$$

Example 7.6. *Given integers $a_1, \dots a_n$, the set of solutions of the diophantine equation*

$$\{(m_1, \dots m_n) \mid a_1 m_1 + \dots a_n m_n = 0\}$$

is a subgroup of $\mathbb{Z}^n$.

Example 7.7. *Let $(A, *, e)$ be an Abelian group. Let $a \in A$, then the set of all powers $\{a^n \mid n \in \mathbb{Z}\}$ is a subgroup called the subgroup generated by a. The previous example, $n\mathbb{Z}$ is just the subgroup of $\mathbb{Z}$ generated by n.*

We can generalize this construction, but first we switch to additive notation, since it makes it easier to see what's going on.

Lemma 7.8. *Given a collection of elements $a_1, a_2, \dots a_k$ of an Abelian group $(A, +, 0)$, the set*

$$S = \{n_1 a_1 + n_2 a_2 + \dots n_k a_k \mid n_i \in \mathbb{Z}\}$$

is a subgroup called the subgroup generated by $a_1, a_2 \dots a_k$.

Proof. $0 = 0a_1 + \dots 0a_k \in S$. Given two elements $x, y \in S$, write them as

$$x = n_1 a_1 + \dots n_k a_k$$

and

$$y = m_1 a_1 + \dots m_k a_k$$

Then

$$x + y = (n_1 + m_1)a_1 + \dots (nk + m_k)a_k \in S$$

and

$$-x = -n_1 a_1 - \dots - n_k a_k \in S$$

□

Theorem 7.9. *Any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n\mathbb{Z}$.*

Proof. Let $S \subseteq \mathbb{Z}$ be a subgroup. If $S = \{0\}$ then we can take $n = 0$. So assume that S contains a nonzero element a. We can assume that $a > 0$, since otherwise we can replace it by $-a \in S$. Therefore the set of strictly positive elements of S is nonempty. Let n be the least such. We will prove that any $x \in S$ is divisible by n. If x is nonnegative, then $x = qn + r$ with $0 \leq r < n$. But $qn = n + n + \dots n \in S$. Therefore $r = x - qn \in S$. It follows that $r = 0$, otherwise r would contradict the minimality of n. So n divides x. If x is negative, then the previous argument shows that n divides $-x$, so it also divides x. □

7.10 Exercises

1. Which of the following are subgroups of $\mathbb{Z}_6$? $A = \{0, 1, 5\}$, $B = \{0, 3\}$, $C = \{0, 2, 4\}$

2. Write down all subgroups of $\mathbb{Z}_4$.

3. Check that example 7.6 is a subgroup.

4. Let $a, b \in \mathbb{Z}$ be nonzero integers with $gcd(a, b) = 1$. Prove that the subgroup $S = \{am + bn = 0 \mid (m, n) \in \mathbb{Z}^2\}$ is generated by $(b, -a)$ with the following steps: We know $ax + by = 1$ has a solution with $x, y \in \mathbb{Z}$. Suppose that $(m, n) \in S$.

   a) Multiply $am + bn = 0$ by x, and after some algebra conclude that $m = bm'$ for some integer m'.

   b) By a similar argument conlcude that $n = an'$ for integer n'.

   c) Substitute these back into the previous equation.

5. Let $a, b \in \mathbb{N}$, prove that the subgroup $S = \{am + bn \mid m, n \in \mathbb{Z}\}$ generated by a, b equals $c\mathbb{Z}$ where $c = gcd(a, b)$.

Chapter 8

Commutative Rings

The set of integers $\mathbb{Z}$ has two interesting operations: addition and multiplication, which interact in a nice way.

Definition 8.1. *A commutative ring consists of a set R with elements $0, 1 \in R$, and binary operations $+$ and $\cdot$ such that:*

1. *$(R, +, 0)$ is an Abelian group*
2. *$\cdot$ is commutative and associative with 1 as the identity: $x \cdot y = y \cdot x$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $x \cdot 1 = x$.*
3. *$\cdot$ distributes over $+$: $x \cdot (y + z) = x \cdot y + x \cdot z$.*

Example 8.2. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual operations are all commutative rings.*

Example 8.3. *$\mathbb{Z}_n$ is in fact a commutative ring. The addition has been discussed already. The product is the $mod\, n$ product*

$$x \odot y = xy \, mod \, n$$

Since the symbols $\oplus$ and $\odot$ are fairly cumbersome, we will usually use ordinary notation with the understanding that we're using $mod\, n$ rules. For example, we write $11 \cdot 9 + 11 \cdot 13$ instead of $(11 \odot 9) \oplus (11 \odot 13)$. When doing calculations by hand, the congruence symbol is very useful. For example, to see that

$$11 \cdot 9 + 11 \cdot 13 = 2 = 11 \cdot (9 + 13)$$

in $\mathbb{Z}_{15}$, we can write:

$$11 \cdot 9 + 11 \cdot 13 \equiv_{15} 99 + 143 \equiv_{15} 9 + 8 \equiv_{15} 2.$$

$$11 \cdot (9 + 13) \equiv_{15} 11 \cdot 7 \equiv_{15} 2.$$

To evaluate this in Maple, just type $11 * 9 + 11 * 13 \, mod \, 15$;.

To get a better feeling for this, we can have Maple generate the addition and multiplication tables for $\mathbb{Z}_n$ with the following code:

```
tables := proc(n::posint)
 local A,B,i,j;
 A := matrix(n+1,n+1);
 B := matrix(n+1,n+1);
 for i from 0 to n-1 do
   for j from 0 to n-1 do
    A[i+2,j+2] := i+j mod n;
    B[i+2,j+2] := i*j mod n;
   od;
  od;
 A[1,1] := `+`;
 B[1,1] := `.`;
 for i from 0 to n-1 do
   A[1,i+2] := i;
   A[i+2,1] := i;
   B[1,i+2] := i;
   B[i+2,1] := i;
 od;
 print(A,B);
 end;
```

To get the tables for $\mathbb{Z}_8$, type:

```
> tables(8);
```

$$\begin{bmatrix} + & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ 2 & 2 & 3 & 4 & 5 & 6 & 7 & 0 & 1 \\ 3 & 3 & 4 & 5 & 6 & 7 & 0 & 1 & 2 \\ 4 & 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\ 5 & 5 & 6 & 7 & 0 & 1 & 2 & 3 & 4 \\ 6 & 6 & 7 & 0 & 1 & 2 & 3 & 4 & 5 \\ 7 & 7 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}, \begin{bmatrix} . & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 3 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \\ 4 & 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 5 & 0 & 5 & 2 & 7 & 4 & 1 & 6 & 3 \\ 6 & 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\ 7 & 0 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

The output are matrices, which can, with a little imagination, be viewed as tables. Looking at the second table, we can see quite a few zeros which don't come from multiplication by 0. A nonzero element a such $ab = 0$, with $b \neq 0$, is called a zero divisor. The elements $2, 4, 6$ are zero divisors. Zero divisors exibit some strange properties, for example $4 \cdot 1 = 4 \cdot 3$, so one can't cancel the 4. These elements have a more extreme property that they become 0 after multiplying them with themselves enough times:

$$2^3 = 2 \cdot 2 \cdot 2 = 0$$

$$4^2 = 4 \cdot 4 = 0$$
$$6^3 = 0$$

The construction of $\mathbb{C}$ from $\mathbb{R}$ involves adjoining $i = \sqrt{-1}$, and considering all possible expressions $a+bi$ with $a, b \in \mathbb{R}$. This construction can be generalized.

Example 8.4. *Let R be a commutative ring. Define*

$$R[i] = \{a + bi \mid a, b \in R\}$$

with rules

$$(a + bi) + (c + di) = (a + b) + (c + d)i$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

Lemma 8.5. *$R[i]$ is a commutative ring.*

For example, $\mathbb{C} = \mathbb{R}[i]$. The other examples of interest to us is the ring of Gaussian integers $\mathbb{Z}[i]$, and the Gausian field $\mathbb{Q}[i]$. We look at some other cases of this in the exercises.

A polynomial is usually regarded as an expression of the form

$$a_0 + a_1 x + \ldots a_n x^n$$

where a_i are numbers of some sort. We will actually define a polynomial to equal the sequence of its coefficients $(a_0, a_1, \ldots)$, but we will use the x to help us keep track of things.

Example 8.6. *The set of polynomials $\mathbb{C}[x]$ with complex coefficients becomes a commutative ring with*

- 0 *denoting the polynomial* $0 + 0x + \ldots$.
- $1 = 1 + 0x + \ldots$.
- $(a_0 + a_1 x + \ldots) + (b_0 + b_1 x + \ldots) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$
- $(a_0 + a_1 x + \ldots)(b_0 + b_1 x + \ldots) = (a_0 b_0) + (a_1 b_0 + a_0 b_1)x + \ldots$

Most standard identities from high school algebra can be carried out for commutative rings. For example:

Lemma 8.7. *Suppose that R is a commutative ring. Let $-x$ denote the inverse of x in $(R, +, 0)$. Then*

(a) $0 \cdot x = 0$.

(b) $(-1) \cdot x = -x$

Proof. Therefore

$$0 \cdot x + x = 0 \cdot x + 1 \cdot x = x \cdot 0 + x \cdot 1 = x(1 + 0) = x$$

Adding $-x$ to both sides proves (a).

For (b), it is enough, by corollary 3.9, to check that $x + (-1)x = 0$. But

$$x + (-1)x = (1 - 1)x = 0 \cdot x = 0$$

□

8.8 Exercises

1. Prove

   (a) $(x+y)^2 = x^2 + 2xy + y^2$.

   (b) $(x-y)(x+y) = x^2 - y^2$

   hold in any commutative ring R, where we define $x^2 = xx$, $2x = x + x$, and $x - y = x + (-y)$. (Check all the steps.)

2. Write out the addition and multiplication tables for $\mathbb{Z}_2[i] = \{0, 1, i, 1+i\}$. Show that $(1+i)^2 = 0$, which means that it is nilpotent.

3. Find all the zero divisors and nilpotent elements in $\mathbb{Z}_{12}$. If you need it, here's the multiplication table

$$\left[\begin{array}{ccccccccccccc}
. & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
2 & 0 & 2 & 4 & 6 & 8 & 10 & 0 & 2 & 4 & 6 & 8 & 10 \\
3 & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9 \\
4 & 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 \\
5 & 0 & 5 & 10 & 3 & 8 & 1 & 6 & 11 & 4 & 9 & 2 & 7 \\
6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 \\
7 & 0 & 7 & 2 & 9 & 4 & 11 & 6 & 1 & 8 & 3 & 10 & 5 \\
8 & 0 & 8 & 4 & 0 & 8 & 4 & 0 & 8 & 4 & 0 & 8 & 4 \\
9 & 0 & 9 & 6 & 3 & 0 & 9 & 6 & 3 & 0 & 9 & 6 & 3 \\
10 & 0 & 10 & 8 & 6 & 4 & 2 & 0 & 10 & 8 & 6 & 4 & 2 \\
11 & 0 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{array}\right]$$

4. Suppose that $gcd(m, n) \neq 1$. Prove that m is zero divisor in $\mathbb{Z}_n$.

Sequences of "random" numbers are often generated on a computer by the following method: Choose n, a, b, x_0, and consider the sequence

$$x_{i+1} = (ax_i + b) \, mod \, n.$$

This sequence will eventually repeat itself. The period is the smallest k such that $x_{i+k} = x_i$ for all i large enough. Obviously, short periods are less useful.

5. Prove that the period is at most n.

6. Explain why picking a nilpotent in $\mathbb{Z}_n$ would be a bad choice.

Chapter 9

A little Boolean Algebra*

$\mathbb{Z}_2$ is the simplest ring there is, and an interesting one at that. We can view the elements as representing "bits" on a computer or $true/false$ in logic. Let's look at the tables:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Taking $1 = true$ and $0 = false$, the tables imply that $+$ and $\cdot$ are the "exclusive or" and "and" operators respectively. That is, $x + y$ is $true$ exactly when one or the other but not both variables are $true$, while $x \cdot y$ is $true$ if and only if x and y are both true. We introduce, few more symbols: (inclusive)" or" $\vee$, and "not" $\neg$ defined by

$$x \vee y = x + y + xy$$

$$\neg x = x + 1$$

While we're at it, let's introduce the more traditional symbol for "and"

$$x \wedge y = x \cdot y$$

We can now prove standard facts from logic by translating them into commutative ring theory. Note that $\mathbb{Z}_2$ has some special properties which makes the algebra quite simple, namely $2x = 0$ and $x^2 = x$.

Lemma 9.1 (De Morgan). $\neg(x \vee y) = (\neg x) \wedge (\neg y)$

This says, for example, that the negation of "it's a duck or it swims" is "it's not bird and it doesn't swim".

Proof. We'll start at both ends an work toward a common value.

$$\neg(x \vee y) = x + y + xy + 1$$

$$\begin{aligned}(\neg x) \wedge (\neg y) &= (x+1)(y+1) \\ &= xy + x + y + 1\end{aligned}$$

□

The following is the "law of excluded middle", and it is the basis of proof by contradiction.

Lemma 9.2. $(\neg x) \vee x = 1$

Proof.

$$\begin{aligned}(\neg x) \vee x &= (x+1) + x + x(x+1) \\ &= 2x + 1 + x^2 + x \\ &= 1 + 2x \\ &= 1\end{aligned}$$

□

For really complicated Boolean (i. e. $\wedge, \vee, \neg$) expressions, we can have Maple help us out in converting these to polynomials. For example, let's convert both sides of the equation in lemma 9.1.

```
> convert(not (x or y), mod2);
```

$$1 + x + y + x\,y$$

```
> convert((not x) and (not y), mod2);
```

$$1 + x + y + x\,y$$

9.3 Exercises

1. Prove the remaining De Morgan law $\neg(x \wedge y) = (\neg x) \vee (\neg y)$.
2. Prove that $\vee$ is associative.
3. Prove the distributive law $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
4. Check that $\neg(x \wedge (\neg z)) \vee ((z \vee x) \vee (\neg y)) = 1$ either by hand or using Maple.

5. A commutative ring R is called Boolean if $x^2 = x$ holds for each $x \in R$. Prove that $2x = 0$ in any Boolean ring. (Hint: evaluate $(x+1)^2$.) $\mathbb{Z}_2$ is Boolean, for other examples, see below and the exercises of 24. All the results of this section extend to Boolean rings.

6. Let P be the collection of subsets of a fixed set X. Let $0 = \{\}$ denote the empty set and $1 = X$. For $A, B \in P$ define $A \cdot B = A \cap B$ (the interesection), and $A + B$ to be the symmetric difference:

$$A + B = \{x \in X \mid \text{ if either } x \in A \text{ or } x \in B \text{ but not in both } \}$$

Check that $(P, 0, 1, +, \cdot)$ is a Boolean ring.

Chapter 10

Fields

There are actually two Abelian groups associated to a commutative ring R. The first is of course the additive group $(R, +, 0)$. The second is:

Definition 10.1. *A unit in R is an element r with a multiplicative inverse. That is an element $r' \in R$ such that $rr' = 1$. The set of units is denoted by R^*.*

Lemma 10.2. *$(R^*, \cdot, 1)$ is an Abelian group.*

As a consequence the inverse of r is unique if it exists, it is denoted by r^{-1}.

Definition 10.3. *A commutative ring R is a field if $R^* = R - 0$, i.e. every nonzero element has an inverse.*

Example 10.4. *$\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, $\mathbb{Z}$ isn't.*

We say that two integers a, b are relatively prime if $gcd(a, b) = 1$

Theorem 10.5. *$\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid m$ and n are relatively prime$\}$*

Proof. If $gcd(m, n) = 1$, then $mm' + nn' = 1$ or $mm' = -n'n + 1$ for some integers by corollary 6.3. After replacing (m', n') by $(m' + m''n, n' - m'')$ for some suitable m'', we can assume that $0 \leq m' \leq n$. Since have $mm' \, mod \, n = 1$, therefore $mm' = 1$ in $\mathbb{Z}_n$.

The converse follows by reversing these steps. □

Corollary 10.6. *If p is a prime, then $\mathbb{Z}_p$ is a field.*

The Euler function is defined by $\phi(n) = |\mathbb{Z}_n^*|$. It follows that $\phi(p) = p - 1$, for p prime.

For small values of n, then inverse of m in $\mathbb{Z}_n$ can easily be determined by writing out the multiplication table. In Maple, the inverse can be computed as $1/m \, mod \, n$.

Definition 10.7. *A field K has finite characteristic if $nx = x + x \ldots x$ (n times) is zero for all $x \in K$. The characteristic of K is the smallest such n if it is has finite characteristic, or else it is defined to be 0.*

For example, the characteristic of $\mathbb{Q}$ is zero, and the characteristic of $\mathbb{Z}_p$ is p.

Lemma 10.8. *A field K does not have zero divisors. That is $xy = 0$ implies $x = 0$ or $y = 0$.*

Let K be field, then we can form a ring $K[i]$ as in chapter 7. This is a field precisely when K does not already contain a square root of -1:

Lemma 10.9. *$K[i]$ is a field if and only if there is no element $x \in K$ with $x^2 = -1$.*

Proof. We prove one direction, the other is left as an exercise. Suppose that there is no element $x \in K$ with $x^2 = -1$. Let $a+bi \in k[i]$ be nonzero, this means that $a \neq 0$ or $b \neq 0$. We claim that $a^2 + b^2 \neq 0$, so that it has an inverse in K. Suppose that this is zero. If $a = 0$ then $b^2 = 0$ implies $b = 0$ by lemma 10.8. But this will contradict the hypothesis. Since $a \neq 0$, we get $a^2 = -b^2$ which implies $(b/a)^2 = -1$, and this contradicts the original supposition. Therefore $a^2 + b^2 \neq 0$ as claimed. It can be checked that the following formula gives the inverse.

$$(a + bi)^{-1} = (a - bi)(a^2 + b^2)^{-1}$$

□

Example 10.10. *It follows that the Gaussian field $\mathbb{Q}[i]$ is a field.*

Example 10.11. *$\mathbb{Z}_p[i]$ is a field if and only if $x^2 \equiv_p -1$ has no integer solutions*

10.12 Exercises

1. Show that $1, -1, i, -i$ are the only units in $\mathbb{Z}[i]$.
2. Find a formula for $\phi(p^2)$, where p is a prime.
3. Find a formula for $\phi(pq)$, where p, q are primes.
4. Find a formula for 2^{-1} in $\mathbb{Z}_p$ where p is an odd prime. Prove it.
5. Compute $(p-1)^{-1}$ (using Maple if necessary) in $\mathbb{Z}_p$ for $p = 3, 5, 7, 11, 13$. Do you notice a pattern? Prove it.
6. Determine for which $p = 2, 3, 5, 7, 11$, $\mathbb{Z}_p[i]$ is a field.
7. Complete the proof of lemma 10.8.
8. Prove that characteristic of a field is either 0 or a prime number.

Chapter 11

Polynomials over a Field

Let K be a field. We can define the commutative ring $R = K[x]$ of polynomials with coefficients in K as in chapter 7. Suppose $f = a_n x^n + \ldots$, where $a_n \neq 0$ and x^n is the highest power of x in f. Then n is called the degree of f, $deg(f)$, and $a_n x^n$ the leading term. A polynomial of degree 0 called a constant polynomial will be regarded as an element of K.

It turns out that R behaves much like $\mathbb{Z}$. In particular, one has a version of the division algorithm:

Theorem 11.1. *Let $f, g \in R$ with $deg(g) \neq 0$. Then there exists unique polynomials q and r, such that*

$$f = qg + r,\ deg(r) < g$$

Proof. The proof is by induction on $deg(f)$. If $deg(f) < deg(g)$, then take $q = 0$ and $r = f$. Otherwise, let ax^n and bx^m be leading coefficients of f and g. Set $q_1 = (ab^{-1})x^{n-m}$ then $f_2 = f - q_1 g$ has degree less than $deg(f)$. Then by induction $f_2 = q_2 g + r$. Therefore $f = (q_1 + q_2)g + r$. □

Given an element $b \in K$, $f(b) \in K$ is defined by substituting b for x in the expression for f. We say b is a root of f if $f(b) = 0$.

Corollary 11.2. *If b is a root of f, then $x - b$ divides f.*

Proof. Then $f = g \cdot (x - b) + r$ where r has degree 0. In other words r is an element of K. Then $r = f(b) = 0$. □

Corollary 11.3. *A nonzero polynomial of degree n can have at most n distinct roots.*

Theorem 11.4 (Lagrange Interpolation). *Given $n + 1$ pairs of elements $a_i, b_i \in k$ with the a_i distinct, there is exactly one polynomial $f \in k[x]$ of degree n such that*

$$f(a_i) = b_i,\ (i = 1, 2, \ldots n + 1)$$

Proof. Let

$$f_j = (x - a_1) \dots (x - a_{j-1})(x - a_{j+1}) \dots (x - a_{n+1})$$

Then

$$f(x) = \sum b_j f_j(a_j)^{-1} f_j(x)$$

will satisfy the above conditions (exercise).

Suppose that g is another degree n polynomial satisfying $g(a_i) = b_i$. Then $f - g$ is a degree n polynomial with $n + 1$ zeros a_i. Therefore $f - g = 0$. $\square$

With the division algorithm in hand, much of the arithmetic of integers can be carried over to polynomials. Given two polynomials, f and g, we say that f divides g if $g = fq$. A common divisor of f and g can be defined as before. A polynomial p is called a greatest common divisor (or gcd) if $deg(p)$ is maximal among all common divisors. It's unique up two multiplication by a nonzero element of K. To break that ambiguity, we will take the gcd to be monic, which means that leading coeff is one. The analogue of corollary 6.3 holds:

Theorem 11.5. *If p is a greatest common divisor of $f, g \in K[x]$, then there exists polynomials $f_1, g_1 \in K[x]$ such that $ff_1 + gg_1 = p$.*

The proof, which is a modification of the previous one, leads to an algorithm which can easily be implemented in Maple (when $K = \mathbb{Q}$).

```
f1 := (f,g) ->
 if (g=0) then
    1/f
 else
    g1(g,rem(f,g,x))
 fi;
g1 := (f,g) ->
 if (g=0) then
    0
 else
    f1(g, rem(f,g,x))-quo(f,g,x)*g1(g,rem(f,g,x))
 fi;
```

In calculus class one learns about partial fractions. There is an implicit assumption that it's possible. Let's prove this in special case.

Corollary 11.6. *Let f, g be nonconstant polyomials with 1 as a gcd. Then there exists polynomials p, q and s with $deg(p) < f$ and $deg(g) < g$ such that*

$$\frac{1}{fg} = s + \frac{p}{f} + \frac{q}{g}$$

Proof. We have $ff_1 + gg_1 = 1$. Therefore

$$\frac{1}{fg} = \frac{g_1}{f} + \frac{f_1}{g}$$

Now apply the division to write $g_1 = q_1 f + r_1$ and $f_1 = q_2 g + r_2$ and substitute above. □

The analogue of a prime number is an irreducible polynomial. Given a polynomial f, and a nonzero element $a \in K$, we can always factor f as $a^{-1}(af)$. We will call this a trivial factorization.

Definition 11.7. *A polynomial $f \in K[x]$ is irreducible if the only factorizations of it are the trivial ones.*

The analogue of the fundamental theorem of arithmetic is the following:

Theorem 11.8. *Any nonconstant polynomial $f \in K[x]$ can be factored into a product of irreducible polynomials. Furthermore if $f = p_1 \dots p_n = q_1 \dots q_m$ are two such factorizations, them $n = m$, and after renumbering there q's, $q_i = a_i p_i$ where $a_i \in K$.*

The concept of irreducibility and factorizations depends very much on the field K. For example $x^2 + 4$ is irreducible as a polynomial over $\mathbb{Q}$ but not over $\mathbb{Q}(i)$ or $\mathbb{C}$. The Maple procedures $irreduc(f)$ and $factor(f)$ can be used to test irreducibility and do factorizations in $\mathbb{Q}[x]$. You can also get it to factor in $\mathbb{Q}(i)[x]$ by typing $factor(f, I)$. Similarly $Irreduc(f)modp$ and $Factor(f)modp$ do this over $\mathbb{Z}_p[x]$.

One of the most important properties of the field of complex numbers is the the fundamental theorem of algebra:

Theorem 11.9. *Any nonconstant polynomial in $\mathbb{C}[x]$ has a root.*

Corollary 11.10. *Any irreducible nonconstant polynomial over $\mathbb{C}$ is linear, i.e. it has degree 1. Consequently any nonconstant polynomial can be factored into a product of linear polynomials.*

Proof. If $f \in \mathbb{C}[x]$ is a nonconstant linear polynomial then it has a root b. Therefore $f = (x - b)g$. Since this must be a trivial factorization g must be a nonzero constant. □

11.11 Exercises

1. Check that the polynomial f given in the proof of theorem 11.4 actually works.

2. Find polynomials $f_1, g_1 \in \mathbb{Q}[x]$ such that $ff_1 + gg_1 = 1$ where $f = x^3 - 2$ and $g = x^2 + x + 1$. Use this to find the partial fraction decomposition of $\frac{1}{(x^3-2)(x^2+x+1)}$ over $\mathbb{Q}$.

3. Prove that $x^n + 1$ is not irreducible over $\mathbb{Q}[x]$ if n is odd.

4. Using Maple, factor $x^n + 1$ in $\mathbb{Q}[x]$ and $\mathbb{Q}(i)[x]$ for $n = 2, 4, 6 \ldots 16$. Can you make a conjecture for when this is irreducible over $\mathbb{Q}[x]$?

5. Using Maple, factor $x^n + 1$ over $\mathbb{Z}_2[x]$ for various n. Use this to find irreducible polymomials of degree $2, 3, \ldots 10$.

6. Modify Euclids proof that there are infinitely many primes to prove that there are infinitely many irreducible polynomials over $\mathbb{Z}_p[x]$ for any prime p.

7. Prove that any nonconstant irreducible polynomial $f \in \mathbb{R}[x]$ is either linear or quadratic.

   (a) Recall that the conjugate of a complex number is $\overline{a + bi} = a - bi$. Prove that $(x - c)(x - \overline{c}) \in \mathbb{R}[x]$ for any complex number c.

   (b) Prove that for $f \in \mathbb{R}[x]$ and $c \in \mathbb{C}$. $\overline{f(c)} = f(\overline{c})$. In particular, if c is a complex root of f, then so is $\overline{c}$.

   (c) Let $f \in \mathbb{R}[x]$ be a nonconstant irreducible polynomial, factor f over $\mathbb{C}[x]$, and then apply the previous results to prove that f is linear or quadratic.

Chapter 12

Quotients of Abelian groups

Let B be a subgroup of an Abelian group A. Given $a \in A$, define the coset of a to be

$$a * B = \{a * b \,|\, b \in B\}$$

For example $e * B = B$.

Example 12.1. *Let $A = \mathbb{Z}$ and $B = 2\mathbb{Z}$. Then $a + B = 2\mathbb{Z}$ if a is even, and $a + B$ is the set of odd numbers if b is odd.*

We write A/B for the set of all cosets. Although, this may, at first glance, seem like a bizarre thing to do, it will turn out to be a very reasonable construction.

Lemma 12.2. *If $a_1 * B = a_2 * B$ if and only if $a_1 * a_2' \in B$.*

Proof. Let $a_1 * a_2' \in B$. Then for any $b \in B$, $a_1 * b = a_2 * (a_1 * a_2' * b) \in a_2 * B$ which implies $a_1 * B \subseteq a_2 * B$. Also $(a_2 * a_1') = (a_1 * a_2')' \in B$. By an argument similar to the one above $a_2 * B \subseteq a_2 * B$.

Suppose $a_1 * B = a_2 * B$, then $a_1 = a_1 * e = a_2 * b$ for some $b \in B$. Multiplying by a_2' yields $a_1 * a_2' = b$. □

Fix $n \in \mathbb{N}$. Let us denote the coset $a + n\mathbb{Z}$ by $\overline{a}$. These are often called congruence classes. Then:

Corollary 12.3. *$\overline{a} = \overline{b}$ if and only if $a \equiv_n b$.*

This will imply that $\mathbb{Z}/n\mathbb{Z}$ is the "same as" $\mathbb{Z}_n$.

This is left as an exercise. This says that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ as sets. What's missing is the addition rule. We do this now.

Given two subsets X, Y of an Abelian group $(A, *, e)$, let

$$X * Y = \{x * y \,|\, x \in X, y \in Y\}$$

Lemma 12.4. $(a_1 * B) * (a_2 * B) = (a_1 * a_2) * B$.

Proof. $(a_1 * b_1) * (a_2 * b_2) = (a_1 * a_2) * (b_1 * b_2)$ shows that $(a_1 * B) * (a_2 * B) \subseteq (a_1 * a_2) * B$. The reverse inclusion $(a_1 * a_2) * B \subseteq (a_1 * B) * (a_2 * B)$ follows from $(a_1 * a_2) * b = (a_1 * e) * (a_2 * b)$. □

Theorem 12.5. *Let Let B be a subgroup of an Abelian group $(A, *, e)$. Then $(A/B, *, B)$ is an Abelian group.*

Proof. This comes down to the following:

$$(a_1 * B) * (a_2 * B) = (a_1 * a_2) * B = (a_2 * a_2) * B = (a_2 * B) * (a_2 * B)$$

$$(a_1 * B) * [(a_2 * B) * (a_3 * B)] = (a_1 * B) * (a_2 * a_3 * B) = a_1 * (a_2 * a_3) * B$$
$$= (a_1 * a_2) * a_3 * B = [(a_1 * B) * (a_2 * B)] * (a_3 * B)$$
$$(a * B) * (B) = a * B$$
$$(a * B) * (a' * B) = (a * a') * B = B$$

□

This implies that $\mathbb{Z}/n\mathbb{Z}$ is an Abelian group. We will leave it as an exercise that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ as Abelian groups. There is one more very natural example.

Example 12.6. *The circle group is $\mathbb{R}/\mathbb{Z}$. The cosets are of the form $x + \mathbb{Z}$ where $0 \leq x < 1$. We can think of taking the closed interval $[0, 1]$ and gluing the end points to get a circle. The addition law can be described as follows: add two numbers in the usual way, and throw away the part to the left of the decimal point.*

12.7 Exercises

1. Let $A = \mathbb{Z}_6$ and $B = \{0, 3\}$. Check that B is a subgroup, and write down all the cosets in A/B, and write down the addition table.

2. Let us revert to using $\oplus$ for modular addition in $\mathbb{Z}_n$ for this exericise. Prove that $\overline{a} + \overline{b} = \overline{a \oplus b}$ in $\mathbb{Z}/n\mathbb{Z}$.

3. Let B be subgroup of an Abelian group A. Prove that if two cosets $a_1 B$ and $a_2 B$ have a nonempty intersection, then they must coincide.

Chapter 13

Orders of Abelian groups

Given a set X, recall that the number of elements of X (which could be infinity) will be denoted by $|X|$. When X is an Abelian group, $|X|$ is called it's order.

Theorem 13.1 (Lagrange). *Let A be an Abelian group of finite order. Then for any subgroup B, $|A| = |B||A/B|$*

Proof. Since A is finite, there are only a finite number of cosets. Let $A/B = \{e*B, a_1*B, \ldots a_n*B\}$. Every element $a \in A$ lies in one of these cosets, namely $a*A$. Exercise 3 of the previous chapter shows that $A = e*B \cup a_1*B \cup \ldots a_n*B$ is a partition. Therefore by corollary 2.3 $|A| = |e*B| + |a_1*B| + \ldots |a_n*B|$. The map from $B \to a_i*B$ given by $x \mapsto a_i*x$ is one to one and onto since it has an inverse given $y \mapsto a_i y$. Therefore $|a_i*B| = |B|$ which implies that $|A| = |A/B||B|$.

□

Corollary 13.2. *The order of any subgroup divides the order of A.*

The order of an element $a \in A$ is the order of the subgroup generated by a.

Lemma 13.3. *The order of n is the least $n > 0$ such that $a^n = e$.*

Corollary 13.4. *The order of $a \in A$ divides the order of A.*

An Abelian group A is called cyclic if there is an element $a \in A$ (called a generator) such that every element of A is a power of A. For example $\mathbb{Z}_n$ is cyclic with 1 as it is generator.

Lemma 13.5. *If $|A| = p$ is prime then it's cyclic. In fact, every element different from the identity is a generator.*

Proof. The order of $a \in A$ is either 1 or p. If it's 1, $a = e$, otherwise a is a generator. □

Corollary 13.6. $a^{|A|} = 1$

Proof. Write $|A| = mn$ where m is the order of a. Then $a^{mn} = (a^m)^n = e$. $\square$

An important special case is the following:

Lemma 13.7. *(Fermat's little theorem). If p is prime and $0 < a < p$ then $a^{p-1} = 1$.*

This leads to a simple test for compositness (nonprimeness) which we call the Fermat test to the base a.

Corollary 13.8. *If $a^{p-1} \not\equiv 1 \, (mod\, p)$ for some $0 < a < p$ then p is not prime.*

It may seems strange that one even needs a test other than the obvious one of attempting to divide by successive integers. The point is that for very large integers (which arise in applications to cryptography), the obvious test is so slow as to be useless. A more practical method would be to might pick several bases at random. If it passes each Fermat test, then p is "probably" prime, but if it fails once it's definitely composite. Most primality tests used in practice, including Maple's *isprime*, procedure use a more accurate variation of this idea.

Fermat had conjectured that integers of the form $P = 2^{2^n} + 1$ were always prime. This was shown to be false by Euler, when $n = 5$, by explicitly factoring it. Let's test the next one, with $n = 6$, using the above method. In this case $P = 18446744073709551617$ is big enough that Maple will be unable to compute a^{P-1} directly:

```
> P := 2^(2^6)+1:
> 2^(P-1);
```

```
Error, integer too large in context
```

However, we only need a^{P-1} in the ring $\mathbb{Z}_P$, and Maple can do this if we tell it to compute $Power(a, P-1) \, mod\, P$. Trying the Fermat test with base 2 is inconclusive, but base 3 shows us that P isn't prime.

```
> Power(2, P-1) mod P; Power(3,P-1) mod P;
```

$$1$$

$$8752249535465629170$$

13.9 Exercises

1. Calculate the orders of all elements of $\mathbb{Z}_{12}$
2. Show that $\mathbb{Z}_p^*$ is cyclic for $p = 3, 5, 7, 11$.
3. Is $\mathbb{Z}_8^*$ cyclic (explain)?
4. Suppose that n passes the Fermat test to base 2 i.e. $2^{n-1} \equiv 1 \, (mod\, n)$. Prove that n must be odd.

5. Calculate all the integers between 3 and 25 which pass the Fermat test to base 2. Are these all prime? (Use Maple.)

6. Suppose that $a \in \mathbb{Z}_n$, prove that $a^{\phi(n)} \equiv_n 1$ if and only if $a \in \mathbb{Z}_n^*$.

Chapter 14

Linear Algebra over $\mathbb{Z}_p$*

For each integer n, let $V = \mathbb{Z}_p^n$ be set of n-tuple of elements of $\mathbb{Z}_p = \{0, 1, \ldots p-1\}$. Of particular interest for applications, is the case of $p = 2$. One might think of the elements of $\mathbb{Z}_2^n$ as representing strings of bits on a computer. $\mathbb{Z}_p^n$ is an Abelian group with

$$(a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots b_n) = (a_1 + b_1, \ldots a_n + b_n)$$

as one might expect. The order of this group is p^n.

Let $S \subseteq V$ be a subgroup. By Lagrange's theorem $|S|$ must also be a power of p. We will explain this in a different way by borrowing the notion of a basis from linear algebra. Given $N \in \mathbb{Z}_p$ define

$$N(a_1, a_2, \ldots a_n) = (Na_1, Na_2, \ldots Na_n)$$

This is consistent with our earlier notation

$$N(a_1, a_2, \ldots a_n) = (a_1, \ldots a_n) + (a_1, \ldots a_n) + \ldots (a_1, \ldots a_n) \text{ (N times)}$$

A collection of elements $v_1, v_2 \ldots v_k \in V$ is called *linearly independent* if the only solution to

$$a_1 v_1 + a_2 v_2 + \ldots a_k v_k = 0,\ a_i \in \mathbb{Z}_p$$

is

$$a_1 = a_2 = \ldots a_k = 0$$

Recall that $v_1, v_2 \ldots v_k \in S$ generates S if every element $s \in S$ can be written as a sum

$$s = a_1 v_1 + a_2 v_2 + \ldots a_k v_k$$

In this context the word "spans" is also used. A collection of elements $v_1, v_2 \ldots v_k \in S$ is called a *basis* if it is linearly independent and generates S.

Lemma 14.1. *If $v_1, v_2 \ldots v_k \in S$ generate S, then $|S| \leq p^k$. Equality holds if and only if this is a basis.*

Proof. Let $v_1, v_2 \dots v_k \in S$ generate S. Define a function $c : \mathbb{Z}_p^k \to S$ which assigns $a_1 v_1 + \dots a_k v_k \in \mathbb{Z}_p^n$ to the vector $(a_1, \dots a_k) \in \mathbb{Z}_p^k$. The function c is onto, therefore $|S| \leq |\mathbb{Z}_p^k| = p^k$.

Suppose that $v_1, v_2 \dots v_k$ is a basis, and suppose that $c(a_1, \dots a_k) = c(a_1', \dots a_n')$. Then

$$(a_1 - a_1')v_1 + \dots (a_n - a_n')v_n = a_1 v_1 + \dots a_k v_k - (a_1' v_1 + \dots a_k' v_k) = 0$$

By linear independence, this is only possible if $a_i = a_i'$. This proves that c is a one to one correspondence in this case. Therefore $|S| = p^k$.

Suppose that $|S| = p^k$...

□

An application of these ideas is in the construction of (linear) error correcting codes. Suppose a message, which we think of as a string of bits, is to be sent over a noisy medium. The noise causes some of the bits to be flipped to incorrect values. In order to detect those errors and possibly recover the orginal message, we can encode the message so as to add redundent "check" bits. The original message can be viewed as a vector in $\mathbb{Z}_2^k$. The encoded message is vector in a subspace $S \subset \mathbb{Z}_2^N$, and the function c constructed in the above proof can be used to encode the original message. We define the distance $d(u, v)$ between two vectors $u, v \in \mathbb{Z}_2^N$ to be the number of entries of u and v which differ. If u is the original encoded message and v the recieved messages, $d(u, v)$ is the number of errors in transmission. The further the distances between distinct code vectors, the better our chances of detecting/correcting errors.

There remains the problem of finding bases. Here we use the technique of Gauss Jordan elimination. Given a set of vectors

$$v_1 = (a_{11}, a_{12}, \dots a_{1n})$$

$$v_2 = (a_{21}, a_{22}, \dots a_{2n})$$

we arrange them in the rows of a matrix

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & & & \end{pmatrix}$$

We then apply a sequence of the following operations called elementary row operations:

- Interchange rows.
- Multiply all elements of a row a by nonzero element of $\mathbb{Z}_p$.
- Add a multiple of one row to another.

The goal is to get the matrix to reduced echelon form which means:

- The leftmost nonzero entry of any row is 1 (called a leading 1).
- The leading 1 occurs to the right of any leading 1 above it.
- A row consisting of 0's occurs at the bottom of the matrix.
- All entries above a leading 1 are 0. it.

The standard results from linear algebra, in our context, tells us:

Theorem 14.2. *Any matrix A over a field can be taken to a reduced echelon matrix B by a finite sequence of elementary row operations. The nonzero rows of B forms a basis of the sybgroup generated by the nonzero rows of A.*

Corollary 14.3. *Any subgroup of $\mathbb{Z}_p^n$ has a basis.*

Here's an example in $\mathbb{Z}_7$:

$$\begin{pmatrix} 2 & 3 & 0 \\ 4 & 5 & 1 \end{pmatrix} \xrightarrow{4Row1} \begin{pmatrix} 1 & 5 & 0 \\ 4 & 5 & 1 \end{pmatrix} \xrightarrow{Row2-4Row1} \begin{pmatrix} 1 & 5 & 0 \\ 0 & 6 & 1 \end{pmatrix}$$

$$\xrightarrow{6Row1} \begin{pmatrix} 1 & 5 & 0 \\ 0 & 1 & 6 \end{pmatrix} \xrightarrow{Row1-5Row2} \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 6 \end{pmatrix}$$

In Maple, this computation can done by

```
> matrix([[2,3,0], [4,5,1]]);
```

$$\begin{bmatrix} 2 & 3 & 0 \\ 4 & 5 & 1 \end{bmatrix}$$

```
> Gaussjord(%) mod 7;
```

$$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 6 \end{bmatrix}$$

14.4 Exercises

1. The weight of a vector $w(v)$ in $v \in \mathbb{Z}_2^N$ is the distance $d(v, 0)$. Show that $d(u, v) = w(u - v)$.
2. Let $S \subset \mathbb{Z}_2^N$ be a subspace. Prove that the minimum distance between distinct vectors of S is the minimum of weights of nonzero vectors $v \in S$.
3. Let $S \subset \mathbb{Z}_2^6$ be the subspace generated by rows of

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

List all the elements of S. Calculate the minimum distance between distinct vectors of S.

4. Find a basis for the subgroup of $\mathbb{Z}_5^4$ generated by $(1, 2, 3, 4)$ $(2, 3, 0, 1)$, $(0, 0, 1, 0)$ and $(3, 0, 2, 0)$.

Chapter 15

Nonabelian groups

Let's start with definition.

Definition 15.1. *A group consists of a set A with an associative operation $*$ and an element $e \in A$ satisfying*

$$a * e = e * a = a,$$

and such that for every element $a \in A$, there exists an element $a' \in A$ satisfying

$$a * a' = a' * a = e$$

A better title for this chapter would have been *not necessarily Abelian groups*, since Abelian groups are in fact groups.

Lemma 15.2. *An Abelian group is a group.*

Proof. The extra conditions $e * a = a * e$ and $a' * a = a * a'$ follow from the commutative law. □

Before giving more examples, let's generalize some facts about Abelian groups.

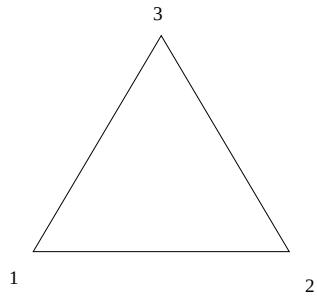
Lemma 15.3. *If $a * b = a * c$ then $b = c$. If $b * a = c * a$ then $b = c$.*

Corollary 15.4. *Given a, there is a unique element a', called the inverse such that $a * a' = a' * a = e$.*

We want give some examples of genuinely nonabelian groups. The next example should already be familiar from linear algebra class (where F is usually taken to be $\mathbb{R}$ or maybe $\mathbb{C}$). We'll say more about this example later on.

Example 15.5. *The set of $n \times n$ invertible (also known as nonsingular) matrices over a field F forms a group denoted by $GL_n(F)$ and called the $n \times n$ general linear group. The operation is matrix multiplication, and the identity element is the identity matrix When $n = 1$, this is just F^* which is Abelian. However, this group is not Abelian when $n > 1$.*

We want to consider a more elementary example next. Consider the equilateral triangle.



We want to consider various motions which takes the triangle to itself (changing vertices). We can do nothing I. We can rotate once counterclockwise.

$$R_+ : 1 \to 2 \to 3 \to 1.$$

We can rotate once clockwise

$$R_- : 1 \to 3 \to 2 \to 1.$$

We can also flip it in various ways

$$F_{12} : 1 \to 2, 2 \to 1, 3 \text{ fixed}$$

$$F_{13} : 1 \to 3, 3 \to 1, 2 \text{ fixed}$$

$$F_{23} : 2 \to 3, 3 \to 2, 1 \text{ fixed}$$

To multiply means to follow one motion by another. For example doing two R rotations takes 1 to 2 and then to 3 etc. So

$$R_+R_+ = R_+^2 = R_-$$

Let's do two flips, F_{12} followed by F_{13} takes $1 \to 2 \to 2$, $2 \to 1 \to 3$, $3 \to 3 \to 1$, so

$$F_{12}F_{13} = R_+$$

Doing this the other way gives

$$F_{13}F_{12} = R_-$$

Therefore this multiplication is not commutative. The following will be proved in the next section.

Lemma 15.6. *$\{I, R_+, R_-, F_{12}, F_{13}, F_{23}\}$ is a group with I as the identity. It is called the triangle group.*

The full multiplication table can be worked out.

$\cdot$	I	F_{12}	F_{13}	F_{23}	R_+	R_-
I	I	F_{12}	F_{13}	F_{23}	R_+	R_-
F_{12}	F_{12}	I	R_+	R_-	F_{13}	F_{23}
F_{13}	F_{13}	R_-	I	R_+	F_{23}	F_{12}
F_{23}	F_{23}	R_+	R_-	I	F_{12}	F_{13}
R_+	R_+	F_{23}	F_{12}	F_{13}	R_-	I
R_-	R_-	F_{13}	F_{23}	F_{12}	I	R_+

where each entry represents the product in the following order

$\cdot$	a	b	$\ldots$
a	$a \cdot a$	$a \cdot b$	$\ldots$

This is latin square (chapter 3), but it isn't symmetric because the commutative law fails. Do all latin squares arise this way? The answer is no. For convenience, let's represent a latin square by an $n \times n$ matrix M with entries $1, \ldots n$. Let's say that there is a group $G = \{g_1, \ldots g_n\}$ with $g = e$ such that M has entry ijth entry k if $g_i * g_j = g_k$. Since $g_1 = e$, we would want the first row and column to be $1, 2, \ldots n$. Such a latin square is called normalized. However, this is still not enough since the associative law needs to hold. I don't know any way to visualize this. Here's a Maple procedure for checking this.

```
assoc := proc(n::posint, M::matrix) i,j,k, associative;
associative := true;
for i from 1 to n do
  for j from 1 to n do
    for k from 1 to n do
      if (M[i,M[j,k]] <> M[M[i,j],k]) then
       associative := false;
       printf("g%d*(g%d*g%d)=g%d\n",i,j,k,M[i,M[j,k]]);
       printf("(g%d*g%d)*g%d=g%d\n\n",i,j,k,M[M[i,j],k]);
      fi;
    od;
  od;
od;
if associative then print("It is associative") fi;
end;
```

Typing $assoc(n, M)$ either tells you if M is associative, or else reports violations to the associative property.

15.7 Exercises

1. 1. Determine the inverse for every element of the triangle group.

2. Prove lemma 15.3.

3. Let $(G, *, e)$ be a group. Prove that the inverse of the product $(x * y)' = y' * x'$.

4. The commutator of x and y is the expression $x * y * x' * y'$. Prove that $x * y = y * x$ if and only if the commutator $x * y * x' * y' = e$.

5. Prove that the multiplication table for a group is always a latin square (see the proof of lemma 3.10 for hints).

6. Test to see if the normalized latin square corresponds to a group:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \\ 3 & 4 & 2 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 3 & 4 & 1 & 2 \end{bmatrix}$$

Chapter 16

Groups of Permutations

We can generalize the example of the triangle group. A permutation of a finite set X is a one to one onto map $f : X \to X$. Write S_X for the set of such permutations. We will be mainly interested in $X = \{1, 2, \ldots n\}$. In this case, we denote the set by S_n. For examples of a permutation in S_4, let

$$f(1) = 2,\ f(2) = 3,\ f(3) = 1,\ f(4) = 4$$

$$g(1) = 1,\ g(2) = 1,\ g(3) = 4,\ g(4) = 3$$

It may be helpful to visualize this:

$$f = \left\{ \begin{array}{ccc} 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 1 \\ 4 & \to & 4 \end{array} \right. \quad g = \left\{ \begin{array}{ccc} 1 & \to & 2 \\ 2 & \to & 1 \\ 3 & \to & 4 \\ 4 & \to & 3 \end{array} \right.$$

Instead of standard functional notation, it'll be more convenient to place functions *to the right* of the argument, as in

$$1 \cdot f = 2$$

(Think of the way you would compute $\sin(x)$ on calculator: you first enter x and then press the sin key.) We get new permutations by composition, in other words following one by another:

$$1 \cdot fg = 2 \cdot g = 1, \ldots$$

and by forming the inverse:

$$2 \cdot f^{-1} = 1$$

We can visualize this by splicing the pictures, or reversing them:

$$fg = \left\{ \begin{array}{ccccc} 1 & \to & 2 & \to & 1 \\ 2 & \to & 3 & \to & 4 \\ 3 & \to & 1 & \to & 2 \\ 4 & \to & 4 & \to & 3 \end{array} \right. = \left\{ \begin{array}{ccc} 1 & \to & 1 \\ 2 & \to & 4 \\ 3 & \to & 2 \\ 4 & \to & 3 \end{array} \right.$$

$$f^{-1} = \begin{cases} 2 & \to & 1 \\ 3 & \to & 2 \\ 1 & \to & 3 \\ 4 & \to & 4 \end{cases}$$

Define the identity function e by $i \cdot e = i$ for each i.

Lemma 16.1. *S_n forms a group under composition with e as the identity. The order (i.e. number of elements) of this group is $n!$.*

Proof. Let $f, g, h \in S_n$ and $i \in \{1, \dots n\}$. Then

$$i \cdot f(gh) = (i \cdot f) \cdot gh = ((i \cdot f) \cdot g) \cdot h = (i \cdot fg) \cdot hi \cdot (fg)h$$

The proves the associative law $f(gh) = (fg)h$.

$$i \cdot fe = (i \cdot f) \cdot e = i \cdot f$$
$$i \cdot ef = (i \cdot e) \cdot = i \cdot f$$

proves that $fe = ef = f$.

Let f^{-1} denote the inverse function. Then

$$i \cdot (ff^{-1}) = (i \cdot f) \cdot f^{-1} = i = i \cdot e$$

$$i \cdot (f^{-1}f) = (i \cdot f^{-1}) \cdot f = i = i \cdot e$$

implies that $ff^{-1}f^{-1}f = e$.

The last statement is a standard counting argument. Given a permutation $f \in S_n$, there are n choices for $1 \cdot f$, $n-1$ choices for $2 \cdot f$... Leading to $n(n-1)\dots 1$ choices for f. □

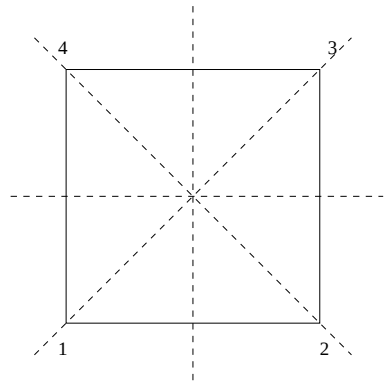
Since the triangle group can be identified with S_3 (exercise), this proves that it's a group. We get more examples of groups by generalizing the definition from chapter 7.

Definition 16.2. *A subset H of a group $(G, *, e)$ is a subgroup if*

1. *$e \in B$.*
2. *B is closed under $*$.*
3. *B is closed under inversion.*

A subgroup of a group is also group.

Example 16.3. *The symmetry group D_4 of the square*



is the subgroup of permutations of the vertices containg all rotations (e.g. $1 \to 2 \to 3 \to 4 \to 1$*) and flips about the dotted lines. (e. g. the vertical flip is* $1 \to 2$*,* $2 \to 1$*,* $3 \to 4$*,* $4 \to 3$*).*

The notation we have been using for writing down permutations is very cumbersome. The most efficient notation is *cycle* notation which is based on the following:

Lemma 16.4. *Let* $p \in S_n$*, then for* $i \in \{1, \ldots n\}$*, the sequence*

$$i \cdot p, i \cdot p \cdot p, \ldots$$

must contain i*.*

The pattern $i \to i \cdot p \to i \cdot p \cdot p \to \ldots i$ is called a cycle, and it's donated by $(i\, i \cdot p \ldots)$. Start with 1, write down the cycle containing it. Pick the next number, say k, not in the previous cycle write down the corresponding cycle. Repeat until all numbers are accounted for. In cycle notation:

$$p = (1\, 1 \cdot p \ldots)(k\, k \cdot p \ldots) \ldots,$$

although normally one omits cycles of length one. In the previous examples,

$$f = (123),\ g = (12)(34),\ fg = (243)$$

It's possible to multiply permutations in Maple. First you have to tell it to load the group theory package:

```
> with(group):
```

Permutations are entered in Maple's version of cycle notation:

```
> f := [[1,2,3]]; g := [[1,2],[3,4]];
```

$$f := [[1, 2, 3]]$$

$$g := [[1, 2], [3, 4]]$$

```
> mulperms(f,g);
```

$$[[2, 4, 3]]$$

The identity would be denoted by [] and the inverse is computed by the command *invperm*.

16.5 Exercises

1. Check that the triangle group coincides with S_3. $R_+ = (123)$ and $F_{12} = (12)$. Check that $F_{12}R_+F_{12} = R_+^2$.

2. Write down all the elements of D_4. Is this an Abelian group?

3. Show by example, that the product of two differents flips in D_4 is a rotation.

4. Let $c = (a_1a_2 \dots a_k)$ be a cycle of length k in S_n. Prove that $c^k = e$.

Chapter 17

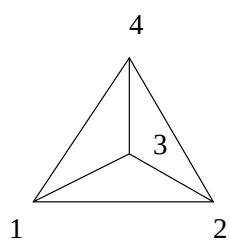
Symmetries of Platonic Solids

There five polyhedra with perfect symmetry. These are the Platonic solids. The last book of Euclid is devoted to their study.

Perfect symmetry means that it is possible to rotate any vertex to any other vertex and any face to any other face. Group theory enters at this point. The symmetry group G of a polyhedron is the group of rotations which takes takes the polyhedron to itself. We will view it as a subgroup of the permutation group of vertices which will be labelled $1, 2, 3, \ldots$. We can partially capture the notion of perfect symmetry by the following:

Definition 17.1. *A subgroup $G \subseteq S_n$ is called transitive if for each pair $i, j \in \{1, \ldots n\}$, there exists $f \in G$ such that $i \cdot f = j$.*

Let us analyse the symmetry of the tetrahedron



which is the simplest Platonic solid.

Let's try and list the elements. There is the identity I. We have two rotations which turning the base and keeping 4 fixed:

$$(123), (132)$$

There are six more rotations which keeps vertices $1, 2$ and 3 fixed:

$$(234), (243), (134), (143), (124), (142)$$

But this isn't all. Since T is a group, we need to include products. For example,

$$(13)(24) = (123)(234)$$

We can do these by hand, but instead we get Maple 8 to produce all possible products of these elements (actually, it suffices to use $(123), (234)$.)

```
> P := permgroup(4, {[[1,2,3]], [[2,3,4]]}):
> elements(P);
```

The output is

$$\{[], [[1,3,4]], [[1,2,3]], [[1,2,4]], [[1,3,2]], [[1,4],[2,3]], [[1,2], [3,4]], [[1,3],[2,4]], [[2,3,4]], [[1,4,2]], [[1,4,3]], [[2,4,3]]\}$$

Certainly, $P \subseteq T$. We want to show these are same. We need a method for computing the number of elements, or order, of T, in advance. First, we make a definitions.

Definition 17.2. *Given subgroup $G \subseteq S_n$ and $i \in \{1, \ldots n\}$, the stabilizer of i, is $\{f \in G \mid i \cdot f = i\}$*

The stablizer of 4 for T is the set

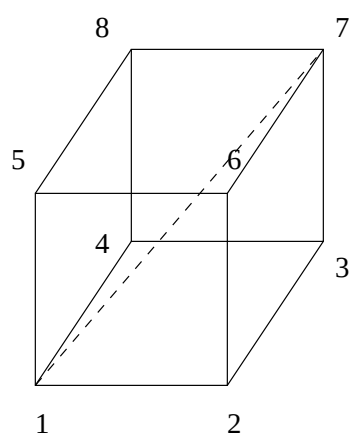
$$\{I, (123), (132)\}$$

with 3 elements.

Theorem 17.3. *Given a transitive subgroup $G \subseteq S_n$, let H be the stabilizer of some element i, then $|G| = n|H|$.*

The proof will be postponed until chapter 19. As a corollary, we get $|T| = (4)(3) = 12$.

Next, consider the cube



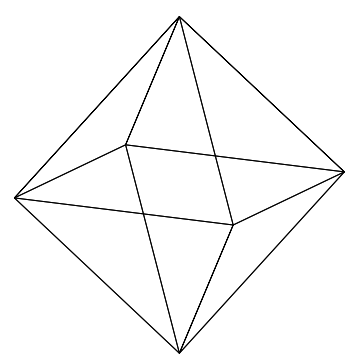
The symmetry group C is the group which takes the cube to itself. This can be viewed as a subgroup of S_8. We need to calculate the stabilizer of 1. Aside from the identity, the only rotations which keep 1 fixed are those with the line joining 1 and 7 as its axis. Thus the stabilizer consists of

$$\{I, (254)(368), (245)(386)\}$$

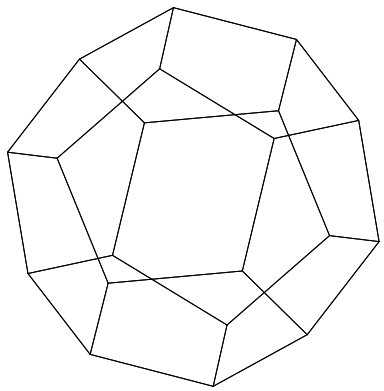
Therefore $|C| = (3)(8) = 24$

17.4 Exercises

1. Show that T is not Abelian.
2. Calculate the order of the symmetry group for the octrahedron



3. Calculate the order of the symmetry group for the dodecahedron



(There are 20 vertices, and 12 pentagonal faces.)

4. Let $G \subset S_n$ be a subgroup. Prove that the stablizer H of an element i is a subgroup of G.

Chapter 18

Counting Problems involving Symmetry*

Group theory can be applied to counting problems invloving symmetry. Here are a few such problems.

Example 18.1. *How many dice can be constructed by labeling the face of a cube by the numbers* $1, \ldots 6$*?*

Example 18.2. *Suppose* 3 *identical decks of* 52 *cards are combined into a big deck. How many* 3 *card hands can be delt out of the big deck?*

Example 18.3. *How many ways can a necklace be constructed with* 2 *black and* 2 *white beads?*

To analyze the first problem, let's first keep track of the order in which cards are dealt. Let's suppose that the kinds of cards are labeled by numbers $1, \ldots 52$. Since we have three decks we can be confident about not running out of kinds. Thus the set of ordered hands can be identified with

$$H = \{(a, b, c) \mid a, b, c = 1, 2 \ldots 52\}$$

The cardinality of this set is 52^3. Of course, we want to disregard order. As first guess, we might think that we should divide this by the number of ways of permuting the cards to get $52^3/6$. Unfortunately, this is not an integer so it doesn't make sense. To explain the correct answer, we will introduce some more group theory.

Definition 18.4. *We say that a group* $(G, *, e)$ *acts on a set* X *if there is an operation* $\cdot : X \times G \to X$ *satisfying:*

1. $x \cdot e = x$.
2. $x \cdot (g * h) = (x \cdot g) \cdot h$

(We're are really defining a right action here, there is also a notion of left action, but we won't need that.)

Definition 18.5. *Given a group G acting on a set X, the orbit of $x \in X$ is the set $x \cdot G = \{x \cdot g \mid g \in G\}$. The set of orbits is denoted by X/G.*

Definition 18.6. *An element x is called a fixed point of g is $x \cdot g = x$.*

Returning to example 18.2. S_3 acts on H by moving the positions of the cards. For example,

$$f = \begin{cases} 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 1 \end{cases}$$

then $(a_1, a_2, a_3) \cdot f = (a_2, a_3, a_1)$. We want to treat two hands as the same if you can permute one to get the other, i.e. if they lie in the same orbit. Therefore our problem is to count the set of orbits H/S_3. If the first two cards are repeated, so $a_1 = a_2$, then (a_1, a_2, a_3) is a fixed point for (12).

Theorem 18.7 (Burnside). *If G is a finite group acting on a finite set X, then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} (\# \text{ of fixed points of } g)$$

This will be proved in the next chapter.

Corollary 18.8. *Suppose that every element other than the identity has no fixed points, then $|X/G| = |X|/|G|$.*

Now, we can solve the problems mentioned earlier. For problem 18.1, we first choose an initial labelling, or marking, of our blank cube. This allows us to talk about the first face, second face and so on. Let X be the set of labellings of the faces of this marked cube. There are 6 choices for the first face, 5 for the second..., therefore there are $6! = 720$ elements of X. $G = C$ is the symmetry group for the cube which has order 24. G acts by rotating the cube. Clearly there are no fixed points for any rotation (other than I). Therefore the number of labellings for a *blank* cube is

$$|X/G| = \frac{720}{24} = 30$$

Next consider problem 18.2. Let H_{ij} be the set of ordered triples (a_1, a_2, a_3) with $a_i = a_j$. This is the set of fix points of (ij). Since there only two free choices, we have

$$|H_{ij}| = 52^2$$

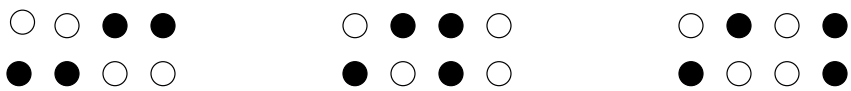
Let H_{123} be the set of triples where all the cards are the same. This is the set of fixed points for (123) and (132). Clearly

$$|H_{123}| = 52$$

Therefore

$$\begin{aligned} H/S_3 &= \frac{1}{6}[|H| + |H_{12}| + |H_{13}| + |H_{23}| + |H_{123}| + |H_{123}|] \\ &= \frac{1}{6}[52^3 + 3(52^2) + 2(52)] \\ &= 24804 \end{aligned}$$

Finally, consider problem 18.3. Let us first arrange the beads in sequence. There are 6 possibilities



and we let X be the set of these. The group in this problem is the symmetry group of the square $D_4 \subset S_4$ which permutes the positions of the beads. All of these are fixed by the identity. The rotations (1234) and (1432) have no fixed points. The element (12)(34) has two fixed points, namely the leftmost sequences in the above diagram. The remaining 4 elements also have two fixed points a piece (exercise). Therefore

$$|X/D_4| = \frac{1}{8}[6 + 5(2)] = 2$$

18.9 Exercises

1. Complete the analysis of problem 18.3.
2. How many necklaces can be constructed using 4 different colored beads?
3. In how many ways can the faces of a tetrahedron be labelled by the numbers $1, 2, 3, 4$?
4. Suppose 2 identical decks of 52 cards are combined into a big deck. How many 3 card hands can be delt out of the big deck?

In the above calculations, certain numbers occured multiple times. This can be explained with the help of the following definition. Two elements $g_1, g_2 \in G$ are *conjugate* if $g_2 = h' * g_1 * h$ for some $h \in G$.

5. Prove that in S_3, (12) is conjugate to (13) and (23), and (123) is conjugate to (132).
6. Suppose that a finite group G acts on a set X. Prove that if g_1 and g_2 are conjugate, then the number of fixed points of g_1 and g_2 are the same.

Chapter 19

Proofs of theorems about group actions

We first prove a strengthened version of theorem 17.3. Given a a group acting a set X, the stabilizer of x is

$$stab(x) = \{g \in G \mid x \cdot g = x\}$$

Theorem 19.1. *Let G be a finite group acting on a set X, then $|G| = |stab(x)||xG|$*

Proof. For each $y \in xG$ let

$$T(y) = \{g \in G \mid x \cdot g = y\}$$

Choose $g_0 \in T(y)$, then the function $f(g) = g * g_0$ maps $stab(x) \to T(y)$. This is a one to one correspondence since it has an inverse $f^{-1}(h) = h * g_0^{-1}$. This implies that $T(y)| = |stab(x)|$.

If $y \neq z$ then $T(y)$ and $T(z)$ must be disjoint, otherwise $y = x \cdot g = z$ for $g \in T(y) \cap T(z)$. Every g lies in some $T(y)$ namely $T(x \cdot g)$. Therefore $T(y)$ is a partition of G. By corollary 2.3,

$$|G| = \sum_{y \in xG} |T(y)| = |xG||stab(x)|$$

□

Given a subgroup H of a group G, a (right) coset is a set of the form $H * g = \{h * g \mid h \in H\}$ for $g \in G$. The set of cosets is denoted by G/H. We can define a right action of G on G/H by

$$(H * g) \cdot \gamma = H * (g * \gamma)$$

This is transitive action which means that there is only one orbit, and the stabilizer $stab(H) = H$ (exercise). Therefore, we obtain an extension of 13.1 to nonabelian groups.

Theorem 19.2 (Lagrange). *Let G be a group of finite order. Then for any subgroup H, $|G| = |H||G/H|$.*

We now prove Burnside's theorem.

Proof. Let

$$C = \{(x, g) \in X \times G \mid x \cdot g = g\}$$

Consider the map $p : C \to G$ given by $p(x, g) = g$. Then an element of $p^{-1}(g)$ is exactly a fixed point of g. Therefore corollary 2.4 applied to p yields

$$|C| = \sum_{g \in G} |p^{-1}(g)| = \sum_{g \in G} (\# \text{ of fixed points of } g) \tag{19.1}$$

Next consider the map $q : C \to X$ given by $q(x, g) = x$. Then $q^{-1}(x) = stab(x)$. Therefore corollary 2.4 applied to q yields

$$|C| = \sum_{x \in x} |p^{-1}(x)| = \sum_{x \in x} |stab(x)|$$

We group the the last sum into orbits

$$C = \sum_{x \in \text{ 1st orbit}} |stab(x)| + \sum_{x \in \text{ 2nd orbit}} |stab(x)| + \dots$$

For each orbit x_0G has $|G|/|stab(x_0)|$ elements by theorem 19.1. Furthermore, for any $x \in x_0G$, we have $|stab(x)| = |stab(x_0)|$. Therefore

$$\sum_{x \in x_0G} |stab(x)| = \sum_{x \in x_0} |stab(x_0)| = \frac{|G|}{|stab(x_0)|} |stab(x_0)| = |G|$$

Consequently

$$|C| = |G| \sum_{\text{orbits}} 1 = |G||X/G|$$

Combining this with equation 19.1 yields

$$|G||X/G| = \sum_{g \in G} (\# \text{ of fixed points of } g)$$

Dividing by $|G|$ yields the desired formula. □

19.3 Exercises

1. Fill in the details in the proof of Lagrange's theorem
   a) Prove that G acts transitively on G/H
   b) Prove that $stab(H) = H$.
2. Prove that if G is a group with $|G|$ a prime, then G is cyclic (compare lemma 13.5).

Chapter 20

Groups of 2×2 Matrices

There is one very important example of a group, that we haven't talked much about yet. This is the group of invertible square matrices over a commutative ring R. To simplify things, we will stick to the 2×2 case. Given two 2×2 matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \; B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

with entries $a, b, \ldots h \in R$, and another element $r \in R$, the products are

$$rA = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix}, \; AB = \begin{pmatrix} a\,e + b\,g & a\,f + b\,h \\ c\,e + d\,g & c\,f + d\,h \end{pmatrix}$$

The identity matrix

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

Lemma 20.1. *If A, B, C are $n \times n$ matrices over a commutative ring R and $r \in R$ then:*

1. $AI = IA = A$.
2. $A(BC) = (AB)C$.
3. $(rA)B = A(rB) = r(AB)$.

Definition 20.2. *An 2×2 matrix A over a commutative ring R is called invertible if there exists an $n \times n$ matrix B over R such that $AB = BA = I$.*

Corollary 20.3. *The set of 2×2 invertible matrices forms a group $GL_2(R)$.*

The inverse of a matrix A is unique if it exists, and is denoted by A^{-1}. There is a criterion for invertibilty for real or complex matrices that one learns in a linear algebra class which works over any commutative ring.

$$det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

Lemma 20.4. *Given 2×2 matrices A, B,*

$$det(AB) = det(A)det(B)$$

Theorem 20.5. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be matrix over a commutative ring R, then A is invertible if and only $det(A) \in R^*$. In this case,*

$$A^{-1} = (det(A))^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Proof. Let $\Delta = det(A)$, and let $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Then an easy calculation gives

$$AB = BA = \Delta I.$$

If $\Delta \in R^*$, then $\Delta^{-1}B$ will give the inverse of A by the above equation.

Conversely suppose A^{-1} exists, then apply lemma 20.4 to $AA^{-1} = I$. This yields $det(A)det(A^{-1}) = 1$. Therefore $det(A) \in R^*$ □

When $K = \mathbb{Z}_p$, $GL_2(K)$ is finite group, so it makes sense to talk about its order. We can apply the techniques from the previous chapter to compute it. Let $V = \mathbb{Z}_p^2$. We let,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

act on $(x, y) \in V$ by multiplying A on the right

$$\begin{pmatrix} x & y \end{pmatrix} A = \begin{pmatrix} ax + cy & bx + dy \end{pmatrix}$$

(For our purposes, ordered pairs are the same thing as 1×2 matrices.)

Theorem 20.6. $|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$

Proof. Let $G = GL_2(\mathbb{Z}_p)$ and $v = (1, 0)$. Then

$$vA = \begin{pmatrix} a & b \end{pmatrix}$$

This vector can be anything but 0. Therefore the orbit vG consisists of $V - \{0\}$. Consequently $|vG| = p^2 - 1$.

The stablizer of v is the set of matrices

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}$$

with nonzero determinant. This means $d \neq 0$. There are p choices for c and $p - 1$ choices for d. Thus the order of the stabilizer is $p(p - 1) = p^2 - p$. The theorem now follows from theorem 19.1.

□

20.7 Exercises

1. Using theorem 20.5 prove that $GL_2(\mathbb{Z}_2)$ consists of the following matrices

$$I, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2. Set $R = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $F = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Verify that $GL_2(\mathbb{Z}_2) = \{I, R, R^2, F, FR, FR^2\}$, and check that it is not abelian.

3. Prove lemma 20.1.

4. Prove lemma 20.4.

Chapter 21

Homomorphisms between groups

When should two groups be considered the same? An unenlightening answer is when they are the same. A more useful answer is that they should be considered the same if we can set up a one to one correspondence between the elements which takes the multiplication table of one to the other. Let's be a little more precise.

Definition 21.1. *Suppose that $(G, *, e)$ and $(H, *, \epsilon)$ are two groups. A group isomorphism between G and H is a one to one correpsondence $f : G \to H$ satisfying $f(g_1 * g_2) = f(g_1) * f(g_2)$ and $f(e) = \epsilon$. It's useful to drop the requirements that f be one to one or onto. We say that a function $f : G \to H$ is a homomorphism if $f(g_1 * g_2) = f(g_1) * f(g_2)$ and $f(e) = \epsilon$.*

We've had examples all along.

Example 21.2. *Let $G \subset H$ be a subgroup. The map $f(g) = g$ is a homorphism.*

Example 21.3. *The map $f : \mathbb{Z} \to \mathbb{Z}_n$ which sends m to $m \bmod n$ is a homomorphism.*

Example 21.4. *The map $\mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ given by $m \mapsto m + n\mathbb{Z}$ is an isomomorphism.*

Example 21.5. *The map $f : \mathbb{Z}_n \to \mu_n$ given by $f(m) = e^{2\pi i m/n}$ is an isomorphism.*

Example 21.6. *Let $(A, *, e)$ be an Abelian group and $n \in \mathbb{Z}$, then nth power map $p : A \to A$ defined by $p(a) = a^n$ is a group homomorphism.*

Example 21.7. *If $B \subseteq A$ is a subgroup of an Abelian group, the map $f : A \to A/B$ taking $a \mapsto a * B$ is a homomorphism by lemma 12.4.*

Example 21.8. *The exponential map $\exp : \mathbb{C} \to \mathbb{C}^*$, where $exp(z) = e^z$ is homomorphism from $(\mathbb{C}, +, 0)$ to $(\mathbb{C}^*, *, 1)$.*

Example 21.9. *Let $\mathbb{R}_+^*$ be the group of positive real numbers. The exponential map* $\exp : \mathbb{R} \to \mathbb{R}_+^*$ *is an isomorphism since it has an inverse given by* $\log$.

Example 21.10. *$det : GL_2(R) \to R^*$ is a homomorphism by lemma 20.4.*

Lemma 21.11. *If $f : G \to H$ is a homomorphism, then the $f(a') = f(a)'$, where a' is the inverse.*

Definition 21.12. *If $f : G \to H$ is a homomorphism, the set $ker(f) = \{g \in G \mid f(g) = \epsilon\}$ is called the kernel, where e is the identity of B. The set $im(f) = \{f(g) \mid g \in G\}$ is called the image.*

Note, that f gives an onto function from $G \to im(f)$ which also denote by f.

Lemma 21.13. *Given a homomorphism $f : G \to H$, $ker(f)$ is a subgroup of G and $im(f)$ is a subgroup of H. f is one to one if and only if $ker(f)$ consists of the identity $\{e\} \subset G$.*

Proof. Certainly $f(e) = \epsilon$ implies that $e \in ker(f)$. If $g_1, g_2 \in ker(f)$, then

$$f(g_1 * g_2) = f(g_1) * f(g_2) = \epsilon * \epsilon = \epsilon$$

and

$$f(g_1') = f(g_1)' = \epsilon$$

Therefore $ker(f)$ is closed under $*$ and inverses. The proof that $im(f)$ is similar and is left for the exercises.

If f is one to one, then $ker(f) = f^{-1}(\epsilon)$ can contain only one element, and this would have to be e. Conversely, suppose $ker(f) = \{e\}$. Then $f(g_1) = f(g_2)$ would imply that

$$f(g_1 * g_2') = f(g_1) * f(g_2)' = \epsilon$$

Therefore $g_1 * g_2' = e$ which implies that $g_1 = g_2$. □

Corollary 21.14. *A homomorphism $f : G \to H$ is an isomorphism if and only if $ker(f) = \{e\}$ and $im(f) = H$.*

Corollary 21.15. *Let A be an Abelian group, then $\{a \mid a^n = 1\}$ and $\{a^n \mid a \in A\}$ are subgroups.*

Proof. These are the kernel and image of the homomorphism given in example 21.6. □

Proposition 21.16. *If G is a finite group and $f : G \to H$ is a homomorphism, then $|G| = |ker(f)||im(f)|$.*

Proof. Let $K = ker(f)$. By Lagrange's theorem 19.2, it is enough to set up a one to one correspondence between $im(f)$ and G/K. Any element $h \in im(f)$ equals $f(g)$ for some $g \in G$. The set

$$\begin{aligned} f^{-1}(h) &= \{r \in G \mid f(r) = f(g)\} \\ &= \{r \in G \mid f(r * g') = e\} \\ &= \{r \in G \mid r * g' = k \in K\} \\ &= \{r \in G \mid r = k * g \in K * g\} = K * g \end{aligned}$$

is a coset. Conversely, any coset $K * g$ arises this way as $f^{-1}(f(g))$. □

Corollary 21.17. *A be a finite Abelian group, then*

$$|A| = |\{a \mid a^n = e\}||\{a^n \mid a \in A\}|$$

for any positive integer n.

Corollary 21.18. *Let p be an odd prime, then the half the elements of $\mathbb{Z}_p^*$ are squares.*

Group actions can be reinterpreted using homomorphisms.

Lemma 21.19. *Given a group G with an action on a set $X = \{x_1, \dots x_n\}$, define the map $f(g) : \{1, \dots n\} \to \{1, \dots n\}$ by $x_{i \cdot f(g)} = x_i \cdot g^{-1}$. Then $f(g)$ is a permutation, and this defines a homomorphism $f : G \to S_n$.*

Two groups G and H are isomorphic, if there exists and isomomorphism $f : G \to H$. The relation is symmetric and transitive by exercise 8.

Theorem 21.20 (Cayley). *Any finite group $(G, *, e)$ is isomorphic to a subgroup of the permutation group S_n, where $n = |G|$*

Proof. G acts on itself by the rule $x \cdot g = x * g$. Let $G = \{g_1 = e, g_2, \dots g_n\}$ then we get a homomorphism $f : G \to S_n$ as above. Let $H = im(f) \subseteq S_n$. This is a subgroup of S_n and $f : G \to H$ is onto. Suppose that $g \in ker(f)$. Then $f(g)$ is the identity. Therefore,

$$e = g_1 = g_{1 \cdot f(g)} = e \cdot g^{-1}$$

which implies that $g = e$. By lemma 21.13, $f : G \to H$ is one to one, and therefore an isomorphism. □

21.21 Exercises

1. Check example 21.6. What if A was replaced by a nonabelian group?
2. Suppose that A is a cyclic group of order n generated by a. Consider the map $f : \mathbb{Z}_n \to A$ defined by $f(m) = a^m$. Check that this is an isomorphism. Use this to justify examples 21.4 and 21.5.

3. Prove lemma 21.11.

4. Prove that the image of homomorphism is a subgroup.

5. Prove corollary 21.18.

6. Prove lemma 21.19.

7. Prove that if A is an Abelian group, and $f : A \to G$ is an onto homomorphism, then G is also Abelian. In particular, a group is Abelian if it is isomorphic to one.

8. Let $f : G \to H$ be an isomorphism, prove that $f^{-1} : H \to G$ is also an isomorphism. Let $h : H \to K$ be another isomorphism. Prove the composition $hf : G \to K$, defined by $hf(g) = h(f(g))$, is an isomorphism.

9. The 2×2 special linear group $SL_2(R)$ over a commutative ring R is the set of 2×2 matrices with determinat 1. Check that this is a group, and calculate its order, when $K = \mathbb{Z}_p$.

Chapter 22

Groups of order 1 through 8

Now that we have decided that isomorphic groups should be considered the same, it makes sense to ask how many groups are there of a given order, say n. Let's start with $n = 1$. There's only one of course, consisting of the identity and nothing else.

Next comes $n = 2$. In fact, we can deal $n = 2, 3, 5, 7$ at the same time. There is only one apiece. The point is these are prime numbers. We know from the exercises of chapters 19 and 21 that these groups are all cyclic, and such groups are all isomorphic to $\mathbb{Z}_n$.

Let's deal with $n = 4$ next.

Theorem 22.1. *There are only two groups of order* 4*, and they are both abelian.*

Proof. Suppose that $G = \{e, a, b, c\}$ is the group in question with e the identity. The possible orders for a, b, c are 2 or 4. If one of these has order 4, then G is cyclic, so it is isomorphic to $\mathbb{Z}_4$.

Suppose the orders are all 2. This means $a * a = b * b = c * c = e$. Let's consider the possible values for $a * b$. If $a * b = e$, then multiplying by a on the left shows $b = a$ which is impossible. If $a * b = a$ then multiplying by a on the left shows $b = e$ which is impossible. If $a * b = b$ then multiplying by b on the right shows $b = e$ which is impossible. Therefore $a * b = c$. Continuing in this way (exercise) yields a complete multiplication table:

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

This example, which is clearly abelian, is called the Klein 4 group. □

The notion of a product of Abelian groups was introduced as in the exercises of chapter 3. The Klein 4 group can also be described as the product $\mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2^2$. We won't attempt to prove the remaining cases, since we don't really have

the tools. But it is reassuring to know that we have seen many of these examples already.

Theorem 22.2. *There are only two groups of order* 6*:* $\mathbb{Z}_6$ *and* S_6*.*

Theorem 22.3. *There are only* 5 *groups of order* 8*:* $\mathbb{Z}_8$*,* $\mathbb{Z}_2^4$*,* $\mathbb{Z}_2 \times \mathbb{Z}_4$*,* D_4 *and one more.*

The mystery group of order 8 will be described later in chapter 28.

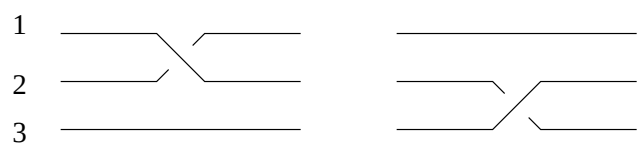
22.4 Exercises

1. Finish all the details of the proof of theorem 22.1.
2. Prove that the groups $\mathbb{Z}_8$, $\mathbb{Z}_2^4$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, D_4 are not isomorphic.
3. In chapter 20, we saw that $GL_2(\mathbb{Z}_2)$ had 6 elements, so it has to be isomorphic to $\mathbb{Z}_6$ or S_3. Which one is it?
4. In the previous exercise, construct an explicit isomorphism.

Chapter 23

The Braid Group*

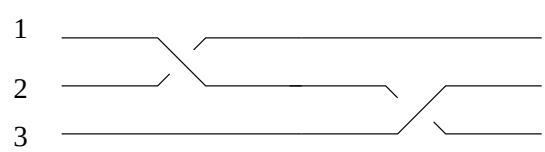
We want to switch gears and take a quick look at the mathematics of braids. This subject is tied up with knot theory and topology. Choose two sets of n points labelled $1, \ldots n$, and connect them by n strings so that every point has exactly one string attached to it. This is called a braid with n strings. Depicted below are 2 braids with 3 strings.



T_{12} T_{32}

Notice we have taken care to indicate when a string crosses *over* another one. The "twist" $T_{i,i+1}$ is the braid where ith string crosses *over* the $(i+1)$st, and $T_{i+1,i}$ means the ith string crosses under. A braid gives rise to a permutation: to see where each element goes, follow the strings.

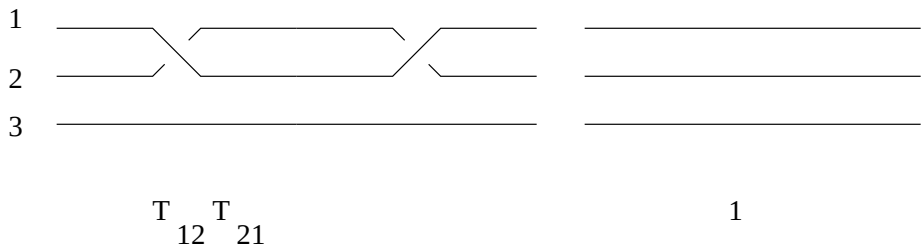
We can "mulitply" two braids by splicing them:



T_{12} T_{32}

This is compatible with the rule for multiplying permutations. It shouldn't be too hard to convince oneself that this is associative. The identity is just

the "unbraid" 1 indicate below. We need to add a rule that two braids are equivalent if you can move the strings without breaking them so to get from the first picture to the second. To put it another way, a braid is equivalent to an unbraid if you can comb through it. Thus two braids indicated below are equivalent



This shows that T_{12} and T_{21} are inverses. In general, we have:

Theorem 23.1 (E. Artin). *The set of braids on n strings considered up to equivalence forms a group B_n. The map $f : B_n \to S_n$ which assigns a permutation to a braid is a homomorphism.*

The first nontrivial case is B_2. Here we have a complete description

Lemma 23.2. *The map $\mathbb{Z} \to B_2$ which sends $n \to T_{12}^n$ is an isomorphism of groups.*

For $n > 2$, B_n is more mysterious. The key step in understanding it, is to find a system of generators. Let's take a look at the permutation group first.

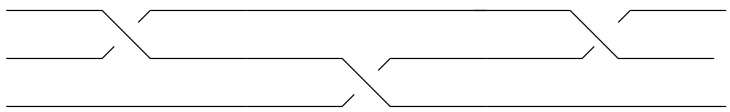
Theorem 23.3. *Any permutation in S_n is a product of the permutations* $(12), (23), \ldots (n-1, n)$.

This can be done in several ways.

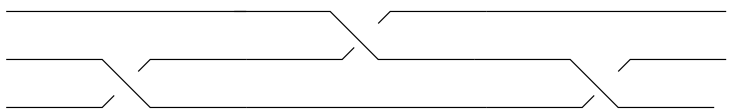
$$(13) = (12)(23)(12) = (23)(12)(23)$$

These results extend to the braid group.

Theorem 23.4 (E. Artin). *The twists $T_{i,i+1}$ generate B_n. In other words, any braid in B_n is a product of a finite number of twists $T_{i,i+1}$ and their inverses. These satisfy the braid relations $T_{i,i+1}T_{i+1,i+2}T_{i,i+1} = T_{i+1,i+2}T_{i,i+1}T_{i+1,i+1}$: (see figure below).*



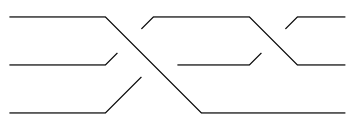
$T_{12}\ T_{23}\ T_{12}$



$T_{23}\ T_{12}\ T_{23}$

23.5 Exercises

1. Prove that B_n is nonabelian when $n > 2$. (Hint: use the map to S_n).
2. Check theorem 23.3 for S_3.
3. Decompose:



   into a product of twists.
4. Prove that $(T_{12}T_{23})^3$ equals $(T_{12}T_{23}T_{12})^2$.

Chapter 24

The Chinese remainder theorem

Definition 24.1. *A map of commutative rings $f : R \to S$ is a ring homomorphism if it's a group homomorphism from $(R, +, 0)$ to $(S, +, 0)$, which also satisfies $f(1) = 1$ and $f(r_1 * r_2) = f(r_1) \cdot f(r_2)$. A ring homomorphism is called an isomorphism if it is one to one and onto.*

Example 24.2. *Let $\mathbb{Z} \to \mathbb{Z}_n$ be given $x \mapsto x \bmod n$ is a ring homorphism.*

Example 24.3. *Let K be a field, and $a \in K$. The map $ev_a : K[x] \to K$ defined by $ev_a(f(x)) = f(a)$ is a ring homomorphism.*

We can refine this a bit.

Lemma 24.4. *Suppose that $n|m$ then $\mathbb{Z}_m \to \mathbb{Z}_n$ given by $x \mapsto x \bmod n$ is a ring homorphism.*

Definition 24.5. *Given two or more commutative rings $R_1, R_2, \ldots$, their product $R_1 \times R_2 \ldots$ becomes a commutative ring with the operations*

$$(r_1, r_2, \ldots) + (r_1', r_2', \ldots) = (r_1 + r_1', r_2 + r_2', \ldots)$$

$$(r_1, r_2, \ldots) \cdot (r_1', r_2', \ldots) = (r_1 \cdot r_1', r_2 \cdot r_2', \ldots)$$

$$\mathbf{0} = (0, 0, \ldots)$$

$$\mathbf{1} = (1, 1, \ldots)$$

A collection of integers $n_1, n_2, \ldots$ is called relatively prime if $gcd(n_i, n_j) = 1$ for all pairs $i \neq j$.

Lemma 24.6. *Suppose that $n_1, n_2, \ldots$ are relatively prime. If an integer x is divisible by all the n_i, then it is divible by their product $n_1 n_2 \ldots$.*

Proof. □

Theorem 24.7 (Chinese remainder theorem). *Suppose that* $n = n_1 n_2 \dots n_r$ *is a product of a relatively prime sequence* $n_1, \dots n_r$ *of natural numbers, then the map*

$$c : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \mathbb{Z}_{n_r}$$

given by

$$c(x) = (x \, mod \, n_1, x \, mod \, n_2, \dots)$$

is an isomorphism of rings.

Proof. It follows from lemma 24.4, that c is a ring homomorphism, and hence a group homomorphism. Suppose that $x \in \ker(c)$. Then x is divisible by all the n_i, and hence by n thanks to the above lemma. Since $x \in \mathbb{Z}_n$, it must be 0. Therefore c is one to one by lemma 21.13. Since

$$|\mathbb{Z}_n| = n = |\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \mathbb{Z}_{n_r}|$$

it follows that c must also be onto. □

Corollary 24.8. *Given integers* $x_1, \dots x_r$*, there is an integer* x *such that* $x \equiv_{n_i} x_i$*.*

Proof. This follows from the fact that c is onto. □

There is something a little unsatisfying about this proof, since it doesn't tell us how to find x. We can give a more constructive argument. Let

$$N_i = n/n_i = n_1 \dots n_{i-1} n_{i+1} \dots n_r$$

Then N_i will be a unit in $\mathbb{Z}_{n_i}$ by theorem 10.5. Therefore, there is an integer N_i' which gives the multiplicative inverse to N_i in $\mathbb{Z}_{n_i}$. In other words $N_i' N_i \equiv_{n_i} 1$. Then setting

$$x = \sum x_j N_i' N_i$$

gives an explicit solution. This quite easy to implement in Maple (here we take $r = 2$):

```
crt := (x1,x2,n1,n2) -> x1*(1/n2 mod n1)*n2 + x2*(1/n1 mod n2)*n1;
```

Or better yet, the following will produce smaller solutions:

```
crt :=
(x1,x2,n1,n2) -> (x1*(1/n2 mod n1)*n2 + x2*(1/n1 mod n2)*n1) mod n1*n2;
```

Lemma 24.9. *Let* $R, R_1, R_2, \dots$ *be commutative rings such that there is an isomorphism*

$$f : R \cong R_1 \times R_2 \times \dots,$$

then the restriction of f *to* R^* *gives an isomorphism*

$$R^* \to R_1^* \times R_2^* \dots$$

Corollary 24.10. *Suppose that $n = n_1 n_2 \ldots n_r$ is a product of a relatively prime sequence, then*

$$c : \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \ldots \mathbb{Z}_{n_r}^*$$

is an isomorphism. In particular,

$$\phi(n) = \phi(n_1)\phi(n_2)\ldots$$

24.11 Exercises

1. Let n be an integer not divisible by 2 or 5. Prove that we can always find a multiple of n such that the last two digits are 99. Do this explicitly for $n = 7$.

2. Suppose that $gcd(n_1, n_2) \neq 1$, does corollary 24.8 hold? (Either prove it, or give an example to show that it fails.)

3. Recall that ring R is Boolean if $x^2 = x$ for all $x \in R$. Prove that the ring of bit vectors $R = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \mathbb{Z}_2$ (n factors) is Boolean.

4. Prove lemma 24.9.

5. Suppose that R and S are commutative rings.

   (a) Prove that the ring $R \times S$ must have a zero divisor.

   (b) Prove that $f : R \to S$ is an isomorphism of commutative rings, then R has a zero divisor if an only if S has a zero divisor.

   (c) Conclude that a field cannot not be isomorphic to a product of two rings.

Chapter 25

Quotients of polynomial rings.

We want to prove a Chinese remainder theorem for polynomials. First, we need analogue of $\mathbb{Z}_n$. Let k be a field, and let

$$f = x^n + a_{n-1}x^{n-1} + \dots a_0$$

be a polynomial. We define $g \; mod \; f$ to be the remainder of g by f. For example, $g \; mod \; f = g$ exactly $deg(g) < n$, and

$$x^n \; mod \; f = -a_{n-1}x^{n-1} \dots - a_1 x - a_0$$

Definition 25.1. *$k[x]/(f)$ is the set of polynomials of degree $n-1$ with 0, 1 and $+$ as usual, but with multiplication $g \odot h = gh \; mod \; f$*

Lemma 25.2. *$k[x]/(f)$ is a commutative ring, and the map $k[x] \to k[x]/(f)$ given by $g \mapsto g \; mod \; f$ is a homomorphism.*

As a first example.

Example 25.3. *$k[x]/(x-a)$ is just k, and $k[x] \to k/(x-a)$ can be identitified with ev_a 24.3.*

In general, the multiplication $k[x]/(f)$ is rigged up so that x^n gets replaced by

$$-a_{n-1}x^{n-1} - \dots - a_1 x - a_0$$

Example 25.4. *$k[x]/(x^2+1)$ is just the set of linear polynomials $\{a+bx\}$, with*

$$(a+bx) \odot (c+dx) = ac + adx + bcx + bdx^2 \; mod \; x^2+1$$

$$= (ac-bd) + (ad+bc)x$$

Aside from a difference in notation, this is just $k[i]$ introduced earlier. In fact, we now have a word for this, $k[i]$ and $k[x]/(x^2+1)$ are isomorphic rings.

We now state a version of the Chinese remainder theorem.

Theorem 25.5. *If $f = (x - a_1)(x - a_2) \dots (x - a_n)$, with a_i distinct, then the map*

$$c : k[x]/(f) \to k \times k \times \dots k \ (n \text{ times})$$

given by $c(g) = (g(a_1), g(a_2), \dots)$ is an isomorphism of rings.

The proof of this similar to the proof of theorem 24.7. Notice that theorem implies the Lagrange interpolation theorem 11.4.

Let us consider, the opposite case where f is doesn't factor. In this case, we have an analogue of corollary 10.6.

Theorem 25.6. *If f is an irreducible polynomial, then $k[x]/(f)$ is a field.*

Proof. If $g \in k[x]/(f)$ is nonzero, then $gcd(g, f) = 1$. By theorem 11.5, there exists a polynomials g_1, f_1 such that $f_1 f + g_1 g = 1$. Therefore $g_1 g \, mod \, f = 1$. The division algorithm implies that $g_1 = fq + r$ with $deg(r) < deg(f)$. Therefore $rg \, mod \, f = g_1 g \, mod \, f = 1$. So r is the inverse of g in $k[x]/(f)$ □

For example, $x^2 - 2$ is irreducible over $\mathbb{Q}$, so $\mathbb{Q}[x]/(x^2 - 2)$ is a field. $x^2 = 2$ so we can identify $x = \sqrt{2}$. $\mathbb{Q}[x]/(x^2 - 2)$ consists of expressions $a + b\sqrt{2}$ with $a, b, \in \mathbb{Q}$. We can express the inverse in these terms by multiplying the numerator and denominator by $a - b\sqrt{2}$

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

In the general the formula for the inverse is complicated. The inverse of g in $\mathbb{Q}[x]/(f)$ can be implemented in Maple by

```
inv := (g,f) -> rem(g1(f,g), f, x);
```

where $g1$ is given after theorem 11.5. For example, $x^3 - 2$ is irreducible over $\mathbb{Q}$, so $\mathbb{Q}[x]/(x^3 - 2)$ is a field. The inverse of $a + bx + cx^2$ can be calculated using Maple as

$$\frac{-x^2\, c\, a + x^2\, b^2 + 2\, x\, c^2 - x\, b\, a + a^2 - 2\, b\, c}{a^3 - 6\, b\, c\, a + 2\, b^3 + 4\, c^3}$$

25.7 Exercises

1. Calculate the inverse of $1 + x$ in $\mathbb{Q}[x]/(x^3 - 5)$.
2. Construct fields $k = \mathbb{Z}_2[x]/(f)$ with 4 and 8 elements. Calculate the order of x in the multplicative group $(k^*, \cdot, 1)$. (Hint: Look at exercise 6 in chapter 11.)
3. Let k be a field. Given $a \in k$, such that $x^2 - a$ has no roots in k, prove that this polynomial is irreducible. The field $k[x]/(x^2 - a)$ is usually denoted by $k[\sqrt{a}]$. Use this construction to prove the existence of a field with p^2 elements for any odd prime p.

Chapter 26

The finite Fourier transform*

Consider the polynomial $x^n - 1 \in \mathbb{C}[x]$. We saw that this factors as

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\dots(x-\omega^{n-1})$$

where $\omega = e^{2\pi i/n}$. Therefore the map

$$\mathcal{F} : \mathbb{C}[x]/(x^n - 1) \to \mathbb{C}^n$$

$$\mathcal{F}(g) = (g(1), g(\omega), \dots, g(\omega^{n-1}))$$

is an isomorphism of rings, where the right side is given the operations of 24.5. $\mathcal{F}$ is often called the finite or discrete Fourier transform. (In spite of the name, these ideas go back to Gauss.) The product on the left is usually called the convolution. In this case, the inverse can be made explicit by the Fourier inversion formula. To simplify formulas, we will index vectors in $\mathbb{C}^n$ so that the first component starts with a_0 or b_0 or ... .

Theorem 26.1 (Fourier Inversion).

$$\mathcal{F}^{-1}(a_0, \dots a_{n-1}) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots b_0$$

where

$$b_m = \frac{1}{n}\sum_{j=0}^{n-1} a_j \omega^{-mj}$$

First we need a lemma

Lemma 26.2. *Let ℓ be an integer*

$$\sum_{m=0}^{n-1} \omega^{\ell m} = \begin{cases} n & \text{if } \ell = 0 \\ 0 & \text{if } \ell = 1, \dots n-1 \end{cases}$$

Proof. If $\ell = 0$ this is clear, so we can assume that $\ell = 1, \ldots n-1$. Recall the formula for summing a geometric series

$$1 + r + r^2 + \ldots r^{n-1} = \frac{r^n - 1}{r - 1}$$

We can apply it when $r = \omega^\ell$ to get

$$\sum_{m=0}^{n-1} \omega^{\ell m} = \frac{\omega^{\ell n} - 1}{\omega^\ell - 1} = 0$$

because $\omega^n = 1$. □

Proof of theorem. Let

$$\mathcal{F}'(a_0, \ldots) = b_{n-1}x^{n-1} + \ldots$$

be given by the formula above. We have to show that

$$\mathcal{F}(\mathcal{F}'(a_0, \ldots)) = (a_0, \ldots)$$

and

$$\mathcal{F}'(\mathcal{F}(g)) = g$$

We will just prove the first part, the second is similar. $\mathcal{F}(\mathcal{F}'(a_1, \ldots))$ is a vector whose kth component is

$$\begin{aligned}
\sum_m b_m \omega^{km} &= \sum_m (\frac{1}{n} \sum_j a_j \omega^{-mj}) \omega^{km} \\
&= \frac{1}{n} \sum_j a_j (\sum_m \omega^{-mj} \omega^{km}) \\
&= \sum_j a_j (\frac{1}{n} \sum_m \omega^{(k-j)m}) \\
&= a_k
\end{aligned}$$

The last equality follows from lemma 26.2. □

The finite Fourier transform has a number of important applications, made practical by the fact there is a very fast method for computing it and its inverse (see exercise 3). One application that we want to mention is the problem of multiplying two large polynomials f and g together. The usual algorithm is not the most efficient method. If we view f, g as elements of $\mathbb{C}[x]/(x^n - 1)$ for $n > deg(f) + deg(g)$, then it's enough multiply them here (because n is large, the terms won't "wrap around"). The procedure then

1. Compute $\mathcal{F}(f)$ and $\mathcal{F}(g)$.
2. Multiply these (this is relatively quick).
3. Compute the inverse transform.

Similar techniques are available for multiplying large integers, and these are much than usual method that one learns in school. See [8, 4.3.3]

26.3 Exercises

To better appreciate what the Fourier transform is, let us think of $\mathcal{F}$ and $\mathcal{F}^{-1}$ as an operation from vectors $(b_0, \ldots b_{n-1}) \in \mathbb{C}^n$ to vectors in $\mathbb{C}^n$. The kth component of $\mathcal{F}(b_0, b_1 \ldots)$ is

$$\sum_{j=0}^{n-1} b_j \omega^{jk}$$

and the kth component of $\mathcal{F}^{-1}(a_0, \ldots)$ is

$$\frac{1}{n} \sum_{j=0}^{n-1} a_j \omega^{-mj}$$

1. Let $n = 2$, work out explicit formulas for $\mathcal{F}$ and $\mathcal{F}^{-1}$. (If you remember your linear algebra, it might be easier to write the vectors in $\mathbb{C}^n$ as column vectors, and represent $\mathcal{F}$ and $\mathcal{F}^{-1}$ by matrices).

2. Do the same for $n = 4$.

3. Show that when $n = 2m$ is even, $\mathcal{F}(b_0, \ldots)$ can be written as

$$\sum_{j=0}^{m-1} b_{2j} (\omega^2)^{jk} + \omega \sum_{j=0}^{m-1} b_{2j+1} (\omega^2)^{jk}$$

   Since $\omega^2 = e^{2\pi/m}$, this says in effect that

$$\mathcal{F}(b_0, b_1 \ldots b_{n-1}) = \mathcal{F}(b_0, b_2, \ldots b_{2m-2}) + \omega \mathcal{F}(b_1, b_3, \ldots b_{2m-1})$$

   When n is a power of 2, this leads to a recursive procedure for computing $\mathcal{F}$ called the fast Fourier transform.

Chapter 27

Matrix Representations of Groups*

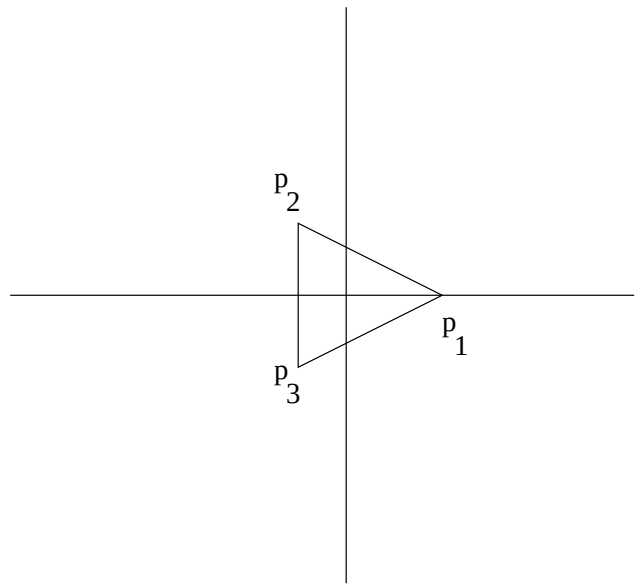
So far we've tried to understand groups by writing down multiplication tables, using permutations and by giving generators. There is one more important technique that we have been ignoring so far, and that is representation of groups by matrices. Given a group G, a complex (real, rational...) n dimensional representation for it is an assigment of an $n \times n$ invertible matrix $R(g)$ to each $g \in G$ such that $R(g_1 g_2)$ is the same as $R(g_1)R(g_2)$. In other words, R is a homorphism from G to $GL_n(\mathbb{C})$. If R is one to one, then R is called *faithful*.

We won't develop the theory. We will be content to just look at a few examples. This will give us an opportunity to revisit some of the earlier material.

Example 27.1. *Write $\omega = e^{2\pi i/n}$. The map $m \mapsto \omega^m$ is a one dimensional representation of $(\mathbb{Z}_n, +, 0)$. More generally, we can consider $m \mapsto \omega^{km}$ for each integer k. These examples were operating behind the scenes in the last chapter.*

Before going on, we have to settle on some conventions. We will identify vectors in $\mathbb{C}^n$ (or $\mathbb{R}^n$ if you prefer) with $1 \times n$ matrices. Given an $n \times n$ matrix A, and a vector $v \in \mathbb{C}^n$, we get a new vector $vA \in \mathbb{C}^n$. From linear algebra class, you're probably used to working with column vectors, and multiplying matrices on the left. However, since we have been applying permutations on the right, it seems less confusing to do things this way.

Example 27.2. *We first encountered S_3 as the symmetry group of an equilateral triangle. This immediately leads to 2 dimensional real representation. Choose equilateral triangle in $\mathbb{R}^2$, such as*



with $p_1 = (1, 0)$, $p_2 = (-1/2, \sqrt{3}/2)$, $p_3 = (-1/2, -\sqrt{3}/2)$. *Solving*

$$p_1 R(12) = p_2,\ p_2 R(12) = p_1$$

and

$$p_2 R(23) = p_3,\ p_3 R(12) = p_2$$

leads to

$$R(12) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix},\ R(23) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Note by theorem 23.3, the values of R can all other permutations can be determined from the above two. Different choices of triangles will lead to different matrices and hence different representations. But are they really so different? At a fundamental level no. We can make this precise. Two n dimensional representations R and R' of the same group G are *isomorphic* if there exists an invertible $n \times n$ matrix M such that $R'(g) = MR(g)M^{-1}$. The representations for different triangles are isomorphic. With a little work, it can be seen that these are isomorphic to a much simpler representation of S_3:

Example 27.3.

$$R(12) = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix},\ R(23) = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

The next example, involving the braid group (chapter 23), definitely does make the group more understandable.

Example 27.4. *Choose a nonzero complex number t, the (reduced) Burau matrices are*

$$\tau_{12} = \begin{pmatrix} -t & 0 \\ -1 & 1 \end{pmatrix}, \ \tau_{23} = \begin{pmatrix} 1 & -t \\ 0 & -t \end{pmatrix}$$

The map $T_{i,i+1} \to \tau_{i,i+1}$ defines a two dimensional representation of B_3.

Notice when $t = 1$, this reduces to the matrices in the previous example. So in this case, we get no more information than we could have by using the homomorphism $B_3 \to S_3$. However, for $t \neq 1$, this definitely gives more (exercise 3). It is easy to implement this in Maple.

```
burau  := proc(lis::list)
local i,B1, B2, p;
 B1 := matrix([[-t, 0], [-1, 1]]);
 B2 := matrix([[1, -t], [0,-t]]);
 p := diag(1,1);
 for i in lis do
   if i[2] <> 0 then
    if i[1] = [1,2] then
      p := evalm(p &* B1^i[2]);
    else
      p := evalm(p &* B2^i[2]);
    fi;
   fi;
 od;
 map(simplify, p);
end;
```

Given a finite product such as $T_{1,2}^2 T_{2,3} T_{1,2}^{-1}$ in B_3, $burau([[[1,2],2],[[2,3],1],[[1,2],-1]])$ will evaluate its image under the Burau representation.

Example 27.5. *Let $e_1 = (1, 0, 0 \ldots 0)$, $e_2 = (0, 1, 0 \ldots 0)$ be the standard basis vectors in $\mathbb{C}^n$. Given $p \in S_n$, let $R(p)$ be the $n \times n$ matrix satisfying $e_i R(p) = e_{i \cdot p}$. This defines an n dimensional representation of S_n. The matrices $R(p)$ are called permutation matrices.*

27.6 Exercises

1. Since example is a representation, and $(123) = (12)(23)$, we should have $p_1 R_{12} R_{23} = p2$, $p_2 R_{12} R_{23} = p3$, and $p_3 R_{12} R_{23} = p1$. Check this.

2. Check the braid relation $\tau_{12}\tau_{23}\tau_{12} = \tau_{23}\tau_{12}\tau_{23}$ holds for any $t \neq 0$.

3. Prove that the element $T_{12} T_{23}^2 T_{12} \in B_3$ is not 1. Note that the image of this element in S_3 is trivial.

4. Work out the permutation matrices for S_3, and verify that it is a representation.

Recall the trace of an $n \times n$ matrix is the sum of its diagonal entries. For finite groups, the following gives a simple test for isomorphism:

Theorem 27.7. *Two representations R and R' of a finite group are isomorphic if and only if $trace(R(g)) = trace(R'(g))$ for all $g \in G$.*

5. Apply this to check that examples 27.2 and 27.3 are isomorphic.

Chapter 28

The ring of Quaternions*

Quaternions were introduced by Hamilton in an attempt to extend complex numbers. Quaterninions can be added and multiplied, and these operations make it a noncommutative ring:

Definition 28.1. *A ring consists of a set R with elements $0, 1 \in R$, and binary operations $+$ and $\cdot$ such that: $(R, +, 0)$ is an Abelian group, $\cdot$ is associative with 1 as the identity, and $\cdot$ distributes over $+$ on the left and right:*

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(y + z) \cdot = y \cdot x + z \cdot x$$

Rings are to commutative rings what nonabelian groups are to Abelian groups. There is one very basic example.

Example 28.2. *The set $M_{nn}(K)$ of $n \times n$ matrices over a field K forms a ring $(M_{nn}(K), +, \cdot, 0, I)$. It is not commutative when $n > 1$.*

The next example is the one of interest to us right now.

Example 28.3. *The ring of quaternions is given by*

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

$$0 = 0 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$$

$$1 = 1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$$

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = (a + a') + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$$

Multiplication is determined by the rules:

$$1 \textit{ is the identity}$$

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$$

$$\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$$

$$\mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Many of the constructions from complex arithmetic carry over to $\mathbb{H}$. We define the conjugate, norm and real and imaginary parts of a quaternion by

$$\overline{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

$$|a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

$$Re(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a$$

$$Im(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

Theorem 28.4. *Let $q \in \mathbb{H}$ then*

(a) $\overline{\overline{q}} = q$.

(b) $\overline{q_1 + q_2} = \overline{q_2} + \overline{q_1}$.

(c) $\overline{q_1 q_2} = \overline{q_2 q_1}$.

(d) $q\overline{q} = |q|^2$.

(e) $|q_1 q_2| = |q_1||q_2|$

The first two statements are easy. For the last two are left as exercises. These are easy to check on a computer, once we implement the basic operations in Maple. We encode the quaternion $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ as a list $[a, b, c, d]$.

```
conj := q -> [q[1], -q[2], -q[3], -q[4]];
```

```
qadd := proc(q1::list, q2::list)
         [q1[1]+q2[1], q1[2]+q2[2], q1[3]+q2[3], q1[4]+q2[4]]
         end;
```

In the next procedure, we exploit the relationship between quaterionic multiplication and the vector cross product to get a short cut. See the exercises.

```
qmult := proc(q1::list, q2::list)
         local vect;
                vect := crossprod(q1[2..4], q2[2..4]);
                vect := evalm(vect + q1[1]*q2[2..4] + q2[1]*q1[2..4]);
                [q1[1]*q2[1] - q1[2]*q2[2]- q1[3]*q2[3]- q1[4]*q2[4],
                        vect[1], vect[2], vect[3]];
        end;
```

In order, to use these, we need to load the linear algebra package before hand by typing $with(linalg)$. Then typing for example $qprod(q, p)$ will calculate the product.

Let $\mathbb{H}^* = \mathbb{H} - \{0\}$. It is easy to see that $q \in \mathbb{H}^*$ if and only if $|q| \neq 0$. As a corollary, we get

Corollary 28.5. $\mathbb{H}$ *forms a group. The inverse*

$$q^{-1} = \frac{\overline{q}}{|q|^2}$$

28.6 Exercises

1. Let $q = 1 + 2\mathbf{i} + 3\mathbf{j}$. Calculate $q' = \overline{q}/|q|^2$ and verify that $qq' = 1$.

2. Prove part (c) of 28.4 (using Maple).

3. Prove part (d).

4. Prove part (e).

5. Check that the set $\{1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ is a subgroup of $\mathbb{H}^*$ and write down the multiplication table for it. This is the missing group in theorem 22.3.

You have probably encountered the dot product $\bullet$ and vector cross product $\times$ on $\mathbb{R}^3$ before. The dot product is an $\mathbb{R}$-valued operation given by

$$(b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \bullet (x\mathbf{i} + y\mathbf{j} + z\mathbf{k}) = bx + cy + dz$$

The cross product is an $\mathbb{R}^3$-valued distributive operation satisfying

$$\mathbf{v} \times \mathbf{w} = -\mathbf{w} \times \mathbf{v}$$

$$\mathbf{i} \times \mathbf{j} = \mathbf{k},\ \mathbf{j} \times \mathbf{k} = \mathbf{i},\ \mathbf{k} \times \mathbf{i} = \mathbf{j}.$$

6. Show that if $\mathbf{v} = (a, b, c)$ and $\mathbf{w} = (x, y, z)$ are identified with the quaternions $b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ and $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$, their quaternionic product

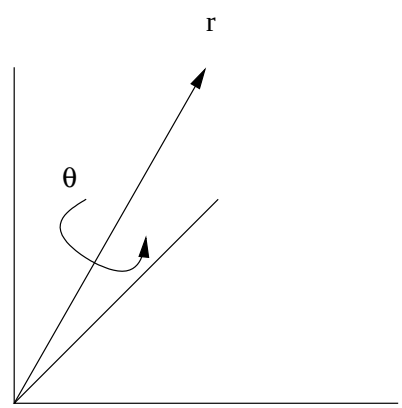
$$\mathbf{v} \cdot \mathbf{w} = \mathbf{v} \bullet \mathbf{w} + \mathbf{v} \times \mathbf{w}$$

7. Is $\times$ associative?

Chapter 29

Quaternions and the Rotation Group*

In this final chapter, we want to turn our attention to the set of all rotations in 3 dimensions. This is certainly important, both mathematically and in terms of the physical applications. Let $\mathbf{r} = (x, y, z)$ be a nonzero vector in $\mathbb{R}^3$ which we may as well take to be a unit vector, which means $x^2+y^2+z^2 = 1$. Let $Rot(\theta, \mathbf{r})$ denote the transformation $\mathbb{R}^3 \to \mathbb{R}^3$ which represents a rotation of angle θ with axis along r using the right hand rule:



$Rot(\theta, \mathbf{r})$ is a linear transformation. Hence we know by linear algebra that it can be represented by a 3×3 matrix. However, this description can be a bit cumbersome. After all, we started with 4 parameters θ, x, y, z, and now we have 9. We will give an alternative based on the ring of quaternions. As a first, step identify $(x, y, z) \in \mathbb{R}^3$ with the quaternion $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$. Define the spin group

$$Spin = \{q \in \mathbb{H} \mid |q| = 1\}$$

The first part of the name comes from physics (as in electron spin), the last part is justified by:

Lemma 29.1. *Spin is subgroup of* $\mathbb{H}^*$.

Proof. This follows from theorem 28.4. □

Lemma 29.2. *If* $q \in Spin$ *and* $v \in \mathbb{H}$ *satisfies* $Re(v) = 0$*, then* $Re(\overline{q}vq) = 0$.

Proof. $Re(v) = 0$ implies that $\overline{v} = -v$. Therefore

$$\overline{\overline{q}vq} = \overline{q}\overline{v}q = -\overline{q}vq$$

(see exercise 1). This implies $Re(\overline{q}vq) = 0$. □

Since we are identifying $\mathbb{R}^3$ with the quaternions q satisfying $Re(q) = 0$, we can define a transformation of $Rot(q) : \mathbb{R}^3 \to \mathbb{R}^3$ by $v \cdot Rot(q) = \overline{q}vq$ for $q \in Spin$. This is a linear transformation, therefore it can be represented by a 3×3 matrix. In fact, this matrix is invertible.

Theorem 29.3. *$Rot(q)$ is a rotation. $Rot(q_1q_2) = Rot(q_1)Rot(q_2)$. For any unit vector $\mathbf{r} = (a, b, c) = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$,*

$$Rot(\cos(\theta/2) - \sin(\theta/2)\mathbf{r})$$

corresponds to $Rot(\theta, \mathbf{r})$.

Corollary 29.4. *R defines a homomorphism from $Spin \to GL_3(\mathbb{R})$.*

The image of Rot is called the rotation group. (Usually this denoted by $SO(3)$. The 3 refers to 3×3 and O to orthogonal.) The rotation group is not isomorphic to the spin group since the kernel of Rot consists of $\{1, -1\}$.

Let's put this stuff to work in an example. Suppose we rotate $\mathbb{R}^3$ counter-clockwise once around the z axis by $90°$, and then around the x axis by $90°$. This can expressed as a single rotation, let's determine it. The first and second rotations given by $Rot(q_1)$ and $Rot(q_2)$ where

$$q_1 = \cos(\pi/4) + \sin(\pi/4)\mathbf{k}$$

$$q_2 = \cos(\pi/4) + \sin(\pi/4)\mathbf{i}$$

Then with the help of the double angle formulas for sin and cos, we get

$$q = q_1q_2 = \frac{1}{2}[1 + \mathbf{i} + +\mathbf{j} + \mathbf{k}]$$

The theorem implies that

$$\frac{Im(q)}{|Im(q)|} = \frac{1}{\sqrt{3}}[\mathbf{i} + \mathbf{j} + \mathbf{k}]$$

is the axis of $Rot(q)$, and the angle of rotation is $\cos^{-1}(1/2)$ which is $60°$.

29.5 Exercises

1. Prove that $\overline{a_1 a_2 \ldots a_n} = \overline{a_n} \ldots \overline{a_2 a_1}$.

2. Repeat the above example in reverse order $(q_2 q_1)$.

3. Prove directly that $|vR(q)| = |v|$. This says that $R(q)$ is orthogonal. This is the first step in the proof of theorem 29.3.

4. Prove directly that if $\mathbf{r} = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$ is a unit vector and α, β satisfy $\alpha^2 + \beta^2 = 1$, then $\mathbf{r} \cdot R(\alpha + \beta\mathbf{r}) = \mathbf{r}$. This is the second step in the proof of the theorem.

Appendix A

Sets and Functions

A set is simply a collection of things called elements. A set can consist of no elements in the case of the empty set $\emptyset$, a finite number of elements, or an infinite number (e.g. $\mathbb{N}$). A finite set can be specified by listing the elements in any order:

$$C = \{red, blue, green\} = \{blue, green, red\}$$

Sometimes we do want to take order into account, instead of a set we use an ordered pair, triple... tuple with $(,)$ instead of $\{,\}$.

$$(red, blue, green) \neq (blue, green, red)$$

It's often convenient to specify a set in terms of the properties that elements satisfy. For example, C can be specified as the set of x such that is a primary color, or

$$C = \{x \mid x \text{ is a primary color}\}$$

$\in$ is elementhood relation, so for example $red \in C$. A subset of C is a set which contains some or all of the elements of C. The relation is denoted by $\subseteq$. For example

$$A = \{red, blue\} \subseteq C$$

Given sets X and Y, we can construct several new sets: the union

$$X \cup Y = \{z \mid z \in X \text{ or } z \in Y\},$$

the intersection

$$X \cap Y = \{z \mid z \in X \text{ and } z \in Y\},$$

the difference

$$X - Y = \{z \mid z \in X \text{ and } z \notin Y\},$$

and the Cartesian product

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}$$

A subset $R \subseteq X \times Y$ is called a *relation* between elements of X and Y. Usually, one writes xRy instead of $(x, y) \in R$. The symbols $=$, $\leq$, $\in$, $\subseteq$ are examples of relations.

A *function* (also called a map, mapping or transformation) $f : X \to Y$ is often thought of some kind process or formula which yields a definite outputs in Y for each input in X. For our purposes, we treat a function as the same as its graph which is a relation $f \subseteq X \times Y$. A relation f is a function if for each $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in f$. Usually, write this as $y = f(x)$, although it will be convenient to use different notation when working with permutations. A function of two variables is just a function from a Cartesian product $f : X_1 \times X_2 \to Y$. For example, addition $a(m, n) = m + n$ is a function $a : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Any expression can be rewritten in functional notation, e.g. $m + (n + r) = a(m, a(n, r))$. In particular, there's nothing special mathematically about *operations*, they're just functions written in an unusual way.

A function $f : X \to Y$ is called *one to one* (or injective) if and only if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. f is called *onto* (or surjective) if for each $y \in Y$, there exists $x \in X$ such that $f(x) = y$. A function is a *one to one correspondence* (or a bijection) if it's both one to one and onto. If f is a one to one correspondence, then the relation

$$f^{-1} = \{(y, x) \mid (x, y) \in f\}$$

is a function $f^{-1} : Y \to X$ called the inverse. Conversely, if f^{-1} is a function then f is a one to one correspondence. Even if f is not a one to one correspondence, we can still define

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

Appendix B

Maple

This appendix describes Maple V5 or higher. I won't get into the details of how you start the program, since that varies from machine to machine. At a basic level, Maple is just a fancy calculator. The nice thing is it does exact arithmetic over $\mathbb{Z}, \mathbb{Q} \ldots$. For example to simplify $(\frac{4}{7} + 3\sqrt{2})^3 - (\frac{4}{7} - 3\sqrt{2})^3$, you can type:

```
> (4/7 + 3*sqrt(2))^3 - (4/7-3*sqrt(2))^3;
```

$$(\frac{4}{7} + 3\sqrt{2})^3 - (\frac{4}{7} - 3\sqrt{2})^3$$

```
> simplify(%);
```

$$\frac{5580}{49}\sqrt{2}$$

Note lines must end with ; (or : to suppress output), % means previous expression, $*$ is the multiplication operator, and ^ is the power operator.

You can use variables. Use := to assign values.

```
> y := 4;
```

$$y := 4$$

```
> (x^2-16)*(x + y)^3;
```

$$(x^2 - 16)(x + 4)^3$$

```
> expand(%);
```

$$x^5 + 12x^4 + 32x^3 - 128x^2 - 768x - 1024$$

```
> factor(%);
```

$$(x - 4)(x + 4)^4$$

Since x has no value, the answer will be a polynomial in x. (It's possible that at some previous stage x had been given a value. Maple has command unassign('x') to deal with this.)

Maple has many data structures analogous to the structures of standard mathematics. For example, finite sets (specified by a sequence enclosed in { }), lists (specified by a sequence enclosed in [ ]) which are like ordered tuples, and matrices (specified for example as $matrix([[a11, a12], [a21, a22]])$).

Maple has many built in functions, such as exp... E.g. to calculate $e^{2\pi i/3}$, type:

```
> exp(2*Pi*I/3);
```

$$-\frac{1}{2} + \frac{1}{2}\, I\, \sqrt{3}$$

You can also create your own functions. For simple functions, you can use the $->$ notation.

```
> cube := x -> x^3;
```

$$cube := x \rightarrow x^3$$

```
> cube(3);
```

$$27$$

We will give a brief sample of some of the more advanced features. For a detailed explanation, you should get hold of a manual or book (e.g. [3]). We will explain how to program the Fibonacci sequence in couple of ways using Maple V (Maple 6 and higher uses a different syntax, but it should be backwards compatible.)

First we implement the obvious recursion

$$fib(n) = \begin{cases} 1 \text{ if } n = 0 \text{ or } n = 1 \\ fib(n-2) + fib(n-1) \text{ otherwise} \end{cases}$$

```
fib := n -> if (n < 2) then
                1
            else
                fib(n-1) + fib(n-2)
            fi;
```

Although this works, it is extremely inefficient. In fact $fib(100)$ would take long time, and might even cause Maple to crash. The problem is that along the way, it computes intermediate values such as $fib(50)$ many times over. The simplest solution is to tell Maple to remember these values so as not to recompute them each time:

```
fib :=proc(n::integer)
option remember;
```

```
if n < 2 then
  1
else
  fib(n-1) + fib(n-2)
fi;
end;
```

It's even more efficient to compute fib by iteration using a loop:

```
fib :=
proc(n::integer)
local f, f1, f2, i;
 if n < 2 then
   1
 else
   f1 := 1;
   f2 := 1;
   f :=1;
   for i from 2 to n do
     f := f1 + f2;
     f2 := f1;
     f1 := f;
   od;
  f;
  fi;
end;
   >  fib(100);
```

$$573147844013817084101$$

For your convenience many of the procedures in these notes are available on the web at http://www.math.purdue.edu/∼dvb/algebra/maplescripts These can simply pasted into a maple session, and then run.

Bibliography

[1] M. Artin, Algebra, Prentice Hall (1991)

[2] T. Bröcker, T. tom Dieck, Representations of compact Lie groups, Springer-Verlag (1985)

[3] A. Heck, Introduction to Maple, Springer-Verlag (1993)

[4] K. Hoffman, R. Kunze, Linear Algebra, Prentice Hall (1971)

[5] K. Ireland, M. Rosen, A classical introduction to modern number theory, Springer-Verlag (1990)

[6] N. Jacobson, Basic Algebra I, W. H. Freeman and Company (1985)

[7] V. Jones, Subfactors and knots, American Math. Soc. (1991)

[8] D. Knuth, The Art of Computer Programming, 3rd ed., Addison-Wesely (1998)

[9] N. Koblitz, A course in number theory and cryptography Springer-Verlag (1987)

[10] J. van Lint, R. Wilson, A course in combinatorics, Cambridge Univ. Press (1992)

[11] H. Weyl, Symmetry, Princeton Univ. Press (1952)