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 $A/B = \{e*B, a_1*B, \dots a_n*B\}$. Every element $a \in A$ lies in one of these cosets, namely $a*A$. Exercise 3 of the previous chapter shows that $A = e*B \cup a_1*B \cup \dots a_n*B$ is a partition. Therefore by corollary 2.3 $|A| = |e*B| + |a_1*B| + \dots |a_n*B|$. 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 $a^{mn} = (a^m)^n = e$. □

An important special case is the following:

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

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 $a \in \mathbb{Z}_n^*$.