Appendix 2A. Congruences in the language of groups

2.6. Further discussion of the basic notion of congruence

Congruences can be rephrased in the language of groups. The integers, $\mathbb{Z}$, form a group,[10] in which addition is the group operation. In exercise 0.11.1 of appendix 0D we proved that the non-trivial, proper subgroups of $\mathbb{Z}$ all take the form $m\mathbb{Z} := \{mn : \ n \in \mathbb{Z}\}$ for some integer $m > 1$, that is, the set of integers divisible by m. The congruence classes (mod m) are simply the *cosets* of $m\mathbb{Z}$ inside $\mathbb{Z}$:

$$0 + m\mathbb{Z}, \ 1 + m\mathbb{Z}, \ 2 + m\mathbb{Z}, \dots, \ (m-1) + m\mathbb{Z},$$

where

$$j + m\mathbb{Z} := \{j + mn : \ n \in \mathbb{Z}\},$$

which is the set of integers belonging to the congruence class $j \pmod m$. Notice that the m cosets of $m\mathbb{Z}$ are disjoint and their union gives all of $\mathbb{Z}$.

The group operation on $\mathbb{Z}$, namely addition, is inherited by the cosets of $m\mathbb{Z}$. For example, as $7 + 11 = 18$ in $\mathbb{Z}$, the same is true when we add together the relevant cosets of $m\mathbb{Z}$ in $\mathbb{Z}$; in other words,[11]

$$(7 + m\mathbb{Z}) + (11 + m\mathbb{Z}) \ = \ (18 + m\mathbb{Z}).$$

This new additive group is the *quotient group*

$$\mathbb{Z}/m\mathbb{Z}.$$

This is the beginning of the theory of quotient groups, which we develop in the next section.

---

[10] See appendix 0D for a discussion of the basic properties of groups.

[11] Throughout, we define the sum of two given sets A and B to be $A + B := \{a + b : \ a \in A, b \in B\}$, that is, the set of elements that can be represented as $a + b$ with $a \in A$ and $b \in B$. Note that an element may be represented more than once.

The reader should be aware that multiplication mod m (and, in particular, how its properties are inherited from $\mathbb{Z}$) does not fit into this discussion of additive quotient groups.

2.7. Cosets of an additive group

Suppose that H is a subgroup of an additive (and so abelian[12]) group G. A *coset* of H in G is given by the set

$$a + H := \{a + h : \ h \in H\}.$$

In Proposition 2.7.1 we will show, as in the example $m\mathbb{Z}$ of the previous section, that the cosets of H are all disjoint and their union gives G.

The *quotient group* G/H has as its elements the distinct cosets $a + H$ and inherits its group law from G, in this case addition, so that

$$(a + H) + (b + H) = (a + b) + H.$$

Proposition 2.7.1. *Let H be a subgroup of an additive group G. The cosets of H in G are disjoint, so that the elements of G/H are well-defined; and the addition law on G/H is also well-defined. If G is finite, then $|H|$ divides $|G|$ and $|G/H| = |G|/|H|$.*

Proof. If $a+H$ and $b+H$ have a common element c, then there exists $h_1, h_2 \in H$ such that $a + h_1 = c = b + h_2$. Therefore $b = a + h_1 - h_2 = a + h_0$ where $h_0 = h_1 - h_2 \in H$ since H is a group (and therefore closed under addition). Now if $h \in H$, then $b+h = a+(h_0+h) \in a+H$, as $h_0+h \in H$, so that $b+H \subset a+H$, and by the analogous argument $a + H \subset b + H$. We deduce that $a + H = b + H$. Hence the cosets of H are either identical or disjoint, which means that they partition G; therefore if G is finite, then $|H|$ divides $|G|$.

This also implies that if $c \in a + H$, then $c + H = a + H$. We wish to show that addition in G/H is well-defined. If $a + H,\ b + H$ are cosets of H, then we defined $(a+H)+(b+H) = (a+b)+H$, so we need to verify that the sum of the two cosets does not depend on the choice of representatives of the cosets. So, if $c \in a + H$ and $d \in b + H$, then there exists $h_1, h_2 \in H$ for which $c = a + h_1$ and $d = b + h_2$. Then $c + H = a + H$ and $d + H = b + H$. Moreover $c + d = a + b + (h_1 + h_2) \in a + b + H$, as H is closed under addition, and so $c + d + H = a + b + H$, as desired. Hence G/H is well-defined, and $|G/H| = |G|/|H|$ when G is finite. □

Example. $\mathbb{Z}$ is a subgroup of the additive group $\mathbb{R}$, and the cosets $a + \mathbb{Z}$ are given by all real numbers r that differ from a by an integer. Every coset $a+\mathbb{Z}$ has exactly one representative in any given interval of length 1, in particular the interval $[0, 1)$ where the coset representative is $\{a\}$, the fractional part of a. These cosets are well-defined under addition and yield the quotient group $\mathbb{R}/\mathbb{Z}$.

The *exponential map* $e : \mathbb{R} \to U := \{z \in \mathbb{C} : \ |z| = 1\}$, from the real numbers to the unit circle, is defined by $e(t) = e^{2i\pi t}$. Since $e(1) = 1$, therefore $e(n) = e(1)^n = 1$ for every integer n. Therefore if $b \in a + \mathbb{Z}$ so that $b = a + n$ for some integer n, then $e(b) = e(a + n) = e(a)e(n) = e(a)$, so the value of $e(t)$ depends only what

[12] A group G is called *abelian* or *commutative* if $ab = ba$ for all elements $a, b \in G$.

coset t belongs to in $\mathbb{R}/\mathbb{Z}$. Therefore we can think of the exponential map as the concatenation of two maps: firstly the natural quotient map from $\mathbb{R} \to \mathbb{R}/\mathbb{Z}$ (that is, $a \to a + \mathbb{Z}$) and then the map $e : \mathbb{R}/\mathbb{Z} \to U$. Picking the representatives $[0, 1)$ for $\mathbb{R}/\mathbb{Z}$, we see that the restricted map $e : [0, 1) \to U$ is 1-to-1.

By a slight abuse of terminology, we let $a \equiv b \pmod 1$, for real numbers a and b, if and only if a and b belong to the same coset of $\mathbb{R}/\mathbb{Z}$.

Exercise 2.7.1. Prove that $a \equiv b \pmod m$ if and only if a/m and b/m belong to the same coset of $\mathbb{R}/\mathbb{Z}$.

Exercise 2.7.2. (a) Prove that $t \equiv \{t\} \pmod 1$ for all real numbers t.
(b) Prove that the usual rules of addition, subtraction, and multiplication hold mod 1.
(c) Show that division is not always well-defined mod 1, by finding a counterexample.

2.8. A new family of rings and fields

We have seen, in Lemma 2.1.1, that the congruence classes mod m support both an additive and multiplicative structure.

Exercise 2.8.1. Prove that $\mathbb{Z}/m\mathbb{Z}$ is a ring for all integers $m \geq 2$.

To be a field, all the non-zero congruence classes of $\mathbb{Z}/m\mathbb{Z}$ would need to have a multiplicative inverse, but this is not the case for all m. For example we claim that 3 does not have a multiplicative inverse mod 15. If it did, say $3m \equiv 1 \pmod{15}$, then multiplying through by 5 we obtain $5 \equiv 5 \cdot 1 \equiv 5 \cdot 3m \equiv 0 \pmod{15}$, which is evidently untrue.

We call 3 and 5 *zero divisors* since they non-trivially divide 0 in $\mathbb{Z}/15\mathbb{Z}$.

Exercise 2.8.2. (a) Prove that if m is a composite integer > 1, then $\mathbb{Z}/m\mathbb{Z}$ has zero divisors.
(b) Prove that $\mathbb{Z}/m\mathbb{Z}$ is not a field whenever m is a composite integer > 1.
(c) Prove that if R is any ring with zero divisors, then R cannot be a field.

An *integral domain* is a ring with no zero divisors. Note that $\mathbb{Z}$ is an integral domain (hence the name) but is not a field.

If R is a commutative ring and $m \in R$, then mR is an additive subgroup of R, and the cosets of mR support a multiplicative structure. To see this, note that if $x \in a + mR$ and $y \in b + mR$, then $x = a + mr_1$ and $y = b + mr_2$ for some $r_1, r_2 \in R$, and so $xy = ab + mr$ where $r = ar_2 + br_1 + mr_1r_2$ which belongs to R, as R is closed under both addition and multiplication. That is, $xy \in ab + mR$. Hence R/mR inherits the multiplicative and distributive properties of R, as well as the identity element $1 + mR$; and so R/mR is itself a commutative ring.

2.9. The order of an element

If g is an element of a given group G, we define the *order* of g to be the smallest integer $n \geq 1$ for which $g^n = 1$, where 1 is the identity element of G. If n does not exist, then we say that g has infinite order (for example, 1 in the additive group $\mathbb{Z}$). We shall explore the multiplicative order of a reduced residue mod m, in detail, in chapter 7.

There is a beautiful observation of Lagrange which restricts the possible order of an element in any finite abelian group.

Theorem 2.2 (Lagrange)**.** *If G is a finite abelian group, then the order of any element g of G divides $|G|$, the number of elements in G. Moreover, $g^{|G|} = 1$.*

Proof. Suppose that g has order n and let $H := \{1, g, g^2, \ldots, g^{n-1}\}$, a subgroup of G of order n. By Proposition 2.7.1 we deduce that $n = |H|$ divides $|G|$. Moreover if $|G| = mn$, then $g^{|G|} = g^{mn} = (g^n)^m = 1^m = 1$. □

Lagrange's Theorem actually holds for any finite group, non-abelian as well as abelian, as we will see in Corollary 7.23.1 of appendix 7D.

Appendices. The extended version of chapter 2 has the following additional appendix:

Appendix 2B. *The Euclidean algorithm for polynomials*, which shows that there is an analogous theory for polynomials.