Group Theory

Lecture 2, Sunday October 30, 2022
Ari Feiglin

2.1 $\mathbb{Z}$ and Introductory Number Theory

Proposition 2.1.1:

For $a, b \in \mathbb{Z}$ where $b \neq 0$ there exist unique $r, q \in \mathbb{Z}$ such that $0 \leq r < b$ and:

$$a = q \cdot b + r$$

Proof:

Let $S = \{n \in \mathbb{Z} \mid b \cdot n \leq a\}$. Since $S \leq |a|$, we can take $q = \max S$. And we define $r = a - q \cdot b$. Then we know by their respective definitions that $a = q \cdot b + r$. we also know that $q \in S$ so $q \cdot b \leq a$, so $r \geq 0$. Assume for the sake of a contradiction that $r \geq b$, but then $a - q \cdot b \geq b$ so $b(q+1) \leq a$, so $q + 1 \in S$, which is a contradiction to q's maximumness $\lightning$.
In order to show uniqueness, suppose $a = q'b + r' = qb + r$ where $r \geq r'$. Then $b(q' - q) = r - r'$, so $b \mid (r - r')$. Since $0 \leq r, r' < b$, it must be that $0 \leq r - r' < b$, so if they are not equal then since b divides their difference, we must have that $r - r' \geq b$, in contradiction. So $r = r'$ and therefore $q = q'$ since $b \neq 0$.

■

We will continue by proving the theorem introduced last lecture:

Theorem 2.1.2:

For every $a, b \in \mathbb{Z}$, $\gcd(a, b)$ is the minimum positive linear combination of a and b.

Proof:

We define

$$\begin{aligned} D &= \{d \in \mathbb{Z} \mid d \mid a, b\} \\ I &= \{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\} \\ I^+ &= \{m \in I \mid m > 0\} \end{aligned}$$

By definition, we know that $d = \gcd(a, b) = \max D$. Let $m = \min I^+$. We know m exists because $I^+ \subseteq \mathbb{N}$. We will show that $\gcd(a, b) = m$. Since $d \mid a, b$, we know that d divides every linear combination of a and b, so $d \mid m$. We know that there exist $q, r \in \mathbb{Z}$ such that:

$$a = q \cdot m + r \qquad 0 \leq r < m$$

Since $m \in I^+$ so $m = \alpha a + \beta b$, and therefore:

$$r = a - q \cdot (\alpha a + \beta b)$$

So r is a linear combination of a and b, so therefore $r \in I$. Suppose $r \neq 0$ then $r > 0$ so $r \in I^+$ and $r < m$ which is a contradiction since m is the minimum. So $r = 0$. Therefore $a \mid m$, and similarly $b \mid m$. Therefore $m \in D$, so $m \leq d$. Since $m > 0$, $d \mid m$ and $m \leq d$, it must be that $m = d$.

■

Notice then that $x \mid a, b$ if and only if $x \mid \gcd(a, b)$. This is because if x divides a and b, then x divides every linear combination of a and b including $\gcd(a, b)$. Since $\gcd(a, b) \mid a, b$, if $x \mid \gcd(a, b)$ then x must divide a and b.
Also recall that last lecture, assuming the result of the theorem above, we showed that a number is prime if and only if it is non-compound. This is true in $\mathbb{Z}$ but not always.

Theorem 2.1.3 (The Fundamental Theorem of Arithmetic):

Every natural number n can be expressed as a unique product of primes, up to order.

This theorem is also called the "prime factorization theorem."

Proof:

We will prove existence inductively. For $n = 1$ this is trivial as it is equal to the empty product. Inductively, if n is prime then it is non-compound so it can only be written as n (which is a product of primes since it is prime). Otherwise, there are p, q such that $m = p \cdot q$, and since p and q have a prime factorization, so does m.
Now we must prove uniqueness. Suppose that for primes p_i and q_j:

$$p_1 \cdot p_2 \cdots p_t = q_1 \cdot q_2 \cdots q_n$$

Since p_1 divides the left and thus the right side, it must divide some q_j. Since q_j is prime and therefore non-compound, $q_j = \pm p_1$, so $q_j = p_1$. Then we can continue inductively on the length of the product.

■

As a side note, notice that there must be infinite primes. Suppose there are finite, let $\{p_1, \ldots, p_n\}$ enumerate them. If we take then $k = p_1 \cdots p_n + 1$, for every i, $p_i \nmid k$ since it divides $k - 1$ but it can't divide 1. So k must be a prime since it can't be factorized by other primes. But then $k = p_i$ for some i, but p_i doesn't divide it, in contradiction, so there must be infinite primes.

2.2 Return to Group Theory

Definition 2.2.1:

Suppose G is a group, then $H \subseteq G$ is a **subgroup** of G's if it is itself a group under the same operation as G. This is denoted $H \leq G$.

Notice then that H is a subgroup of G's if and only if H is non-empty and closed under G's operation (if $a, b \in H$ then $a \circ b \in H$) and under inversion (if $a \in H$, $a^{-1} \in H$). The direction from H being a subgroup to the requirements is trivial. If H satisfies the requirements, then it gets associativity "for free" and $e \in H$ since there is a $a \in H$ and therefore $a^{-1} \in H$ so $a \circ a^{-1} = e \in H$.

Example:

Let $n \in \mathbb{N}_{\geq 1}$, and we define an equivalence relation on $\mathbb{Z}$ as follows:

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

This is obviously symmetric and reflexive, and it is transitive since if $n \mid (a-b), (b-c)$, then $n \mid (a-b+b-c) = (a-c)$. Notice then that if $x \in \mathbb{Z}$, there is some $k \in \{0, \ldots, n-1\}$ such that $x \equiv k \pmod{n}$ since $x = q \cdot n + k$ for some $0 \leq k < n$, so $n \mid (x - k)$, so $x \equiv k \pmod{n}$ as requires. And for $k < j$ for $k, j \in \{0, \ldots, n-1\}$ then $j - k = \{1, \ldots, n-1\}$ so n doesn't divide $j - k$, so they are not equivalent.
We define $\mathbb{Z}_n$ as the partition of $\mathbb{Z}$ under this equivalence relation, $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$, where $[x]$ is the equivalence class of x. We can define an operation on this set by: $[a] + [b] = [a + b]$. This may seem trivial at first, but this is not necessarily well-defined. Suppose $a' \in [a]$ and $b' \in [b]$ then we must show that $[a + b] = [a' + b']$, we will do so by showing $a + b \in [a' + b']$. This is true since $(a' + b') - (a + b) = (a' - a) + (b' - b)$ and since both of these are divisible by n, so is $(a' + b') - (a + b)$, so $[a + b] = [a' + b']$ as required, so the operation is well-defined.
$\mathbb{Z}_n$ under this operation actually forms an abelian group:

- The associativity of this operation comes as a direct consequence of the associativity of integer addition:

$$([a] + [b]) + [c] = [a + b] + [c] = [a + b + c] = [a] + ([b] + [c])$$

- $[0]$ is the identity element since $[a] + [0] = [a + 0] = [a]$ and $[0] + [a] = [0 + a] = [a]$.
- The inverse of $[a]$ is $[-a]$ since $[a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a]$.
- The commutativity of this operation is a direct result of the commutativity of integer addition:

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

Notice then that $\mathbb{Z}_n$ is a group of size n, and therefore for every integer number (larger than 0), there exists a group of that size. This is not the case for other algebraic structures, for example finite fields must have a size of the form p^n for p prime.

Example:

For $\mathbb{Z}_4$ one subgroup is $\{[0],[2]\}$, since $[2]+[2]=[4]=[0]$. In fact other than the trivial group and $\mathbb{Z}_4$ itself, this is the only subgroup.

Definition 2.2.2:

Two groups, $(G,\circ)$ and $(H,\cdot)$ are **isomorphic** if there exists a function:

$$\varphi\colon G \longrightarrow H$$

Such that for every $g_1, g_2 \in G$:

$$\varphi(g_1 \circ g_2) = \varphi(g_1)\cdot\varphi(g_2)$$

This is denoted $G \cong H$. φ is called a **isomorphism**.

Example:

Let us again look at the set $\mathbb{Z}_n$, but this time we will define a new operation:

$$[a]\cdot[b] = [a\cdot b]$$

This is well defined since if $a' \in [a]$, $b' \in [b]$ then notice that:

$$ab - a'b' = b'(a-a') + a(b-b')$$

Since $a-a'$ and $b-b'$ are divisible by n, so is $ab-a'b'$ so $[ab]=[a'b']$, as required.
This is obviously associative since multiplication is (for the same reason it is commutative). And $[1]$ is the identity element since $[1]\cdot[a]=[a]=[a]\cdot[1]$. Therefore $(\mathbb{Z}_n,\cdot)$ is a monoid, but it is not a group. This is because $[0]$ has no inverse, since $[0]\cdot[a]=[0]\neq[1]$. Even if we ignore $[0]$, in some cases other elements will still not have an inverse, take for instance $[2]\in\mathbb{Z}_6$ since 6 does not divide $2n-1$ for any $0\leq n\leq 5$. The same is true for 3 and 4 in fact.

Proposition 2.2.3:

Suppose M is a monoid. We define:

$$\mathcal{U}(M) = \{a \in M \mid a \text{ is invertible}\}$$

Then $\mathcal{U}(M)$ is a group.

Proof:

Associativity comes from the associativity of a monoid, since the identity of a monoid is invertible, it is in $\mathcal{U}(M)$. Since the inverse of an inverse is the original element, if $a\in\mathcal{U}(M)$, so is a^{-1}, and therefore $\mathcal{U}(M)$ is closed under inverses. And since $(a\circ b)^{-1}=b^{-1}\circ a^{-1}$, if $a,b\in\mathcal{U}(M)$, so is $a\circ b$, so $\mathcal{U}(M)$ is closed under multiplication. ■

Notice then that if G is a group, $\mathcal{U}(G)\leq G$.

Example:

$\mathcal{U}((\mathbb{Z}_6,\cdot)) = \{1,5\}$ and it is congruent to $(\mathbb{Z}_2,+)$.

Definition 2.2.4:

We define the **Euler Group** of n to be:

$$\text{Euler}(n) = \mathcal{U}((\mathbb{Z}_n,\cdot))$$

Firstly notice that if $a\equiv b \pmod n$ then $\gcd(n,a)=\gcd(n,b)$, since $b-a=qn$ so every linear combination of a and n is a linear combination of b and n and vice versa.

Proposition 2.2.5:

$[a]$ is invertible in $(\mathbb{Z}_n, \cdot)$ if and only if $\gcd(a, n) = 1$.

Proof:

Suppose $[b]$ is the inverse of $[a]$, then $[ab] = [1]$, that is $ab \equiv 1 \pmod{n}$, so $ab - 1 = qn$, and so $1 = ba - qn$, so 1 is a linear combination of a and n, and it must be the minimum positive linear combination, so $\gcd(a, n) = 1$.
For the converse, suppose $\gcd(a, n) = 1$, then there exists a b and β such that $ba + \beta n = 1$, so $n \mid (ba - 1)$ and by definition $ba \equiv 1 \pmod{n}$. Therefore $[b][a] = [1]$, and since the monoid is associative, $[b]$ is $[a]$'s inverse.

Thus $\mathcal{U}((\mathbb{Z}, \cdot)) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.