Week 3: Group Theory Applications

Anish Kulkarni, Vavilala Chidvilas

Contents

1 Number theory

1.1 Modular arithmetic

- Let n be a positive integer, $a \equiv r \mod n$ means that n divides $a - r$.
- If $a_1 \equiv r_1$ and $a_2 \equiv r_2$, then $a_1 a_2 \equiv r_1 r_2$. Because $a_1 = q_1 n + r_1, a_2 = q_2 n + r_2$, now multiply them and we can see that $a_1 a_2 - r_1 r_2$ is divisible by n.
- The operation "Multiplication modulo n" (let it be *) is defined as : $a * b = r$, where r is such that $ab \equiv r \mod n$ and $0 \leq r \leq n - 1$. (For example if $n = 5$ then $3 \cdot 2 = 1$ as $3 \times 2 = 6$ which is 1 mod 5)

1.2 Bezout's Lemma

Classic Statement: Let a, b be coprime integers, then there exist integers x, y such that $ax + by = 1$.

Equivalent Statement: Let n be a positive integer and a be an integer such that $\gcd(a, n) = 1$, then there exists an x such that $ax \equiv 1 \bmod n$. [10pt]

Proof: We shall prove the classical version and the equivalent statement shall follow directly.
Let $S = \{au + bv : u, v \in \mathbb{Z}, au + bv > 0\}$.
As S is non-empty, it must contain a smallest element say $d = au' + bv'$.
If $d|a$ and $d|b$ then $d = 1$ as they are coprime and we are done. So for the sake of contradiction assume d does not divide atleast one of a and b, say d does not divide a.

Now let $a = dq + r$ where $0 < r < d$ (by Euclid's division lemma)
Then we have $r = a - dq = a - aqu' - bqv' = a(1 - qu') + bqv'$ which is in S contradicting the fact that d was the smallest.
Hence $d = 1$ and we get the required result.

1.3 Exercises (must do to understand next section)

1. Consider $\mathbb{Z}_n = \{0, 1, \cdots, n - 1\}$ and we define the operation to be "addition modulo n". Essentially $a \cdot b = r$ if $a + b \equiv r \bmod n$ and $0 \leq r \leq n - 1$. Check that this is a binary operation on $\mathbb{Z}_n$ and it makes it into a group.
2. Using Bezout's Lemma show that the set of elements x in $\mathbb{Z}_n = \{0, 1, \cdots, n - 1\}$ such that $\gcd(x, n) = 1$ form a group under the operation multiplication modulo n. This group is denoted by $\mathbb{Z}_n^*$
3. If $n = p$ is a prime then show that $\mathbb{Z}_p^* = \{1, 2, \cdots, p - 1\}$

1.4 Fermat's theorem and Euler's theorem

Consider the group $\mathbb{Z}_p^*$ formed by the elements $\{1, 2, 3..., p-1\}$ under the group operation multiplication modulo p (where p is a prime).
From week 2 we know that, the order of an element of a finite group divides the order of that group (that is the number of elements in the group). For any element b of the group $\mathbb{Z}_p^*$, let the order of b be m, i.e $b^m = 1$, and since m divides $p - 1$ (the order of G), hence b^{p-1} is also equal to 1.

1.4.1 Fermat's Little theorem

For any $a \in \mathbb{Z}$ and let p be a prime not dividing a, then p divides $a^{p-1} - 1$, i.e. $a^{p-1} \equiv 1 \mod p$.

Proof: Let $a \equiv r \mod p$ for some $r \in \{1, 2, 3..., p - 1\}$, then $a^{p-1} \equiv r^{p-1} \mod p$, but from above discussion we have $r^{p-1} \equiv 1 \mod p$, hence $a^{p-1} \equiv 1 \mod p$. Thus proved.

Let $\phi(n)$ be the number of positive integers less than n and co-prime to n. Consider the group $\mathbb{Z}_n^*$ (as defined in above exercises), the order of this group is $\phi(n)$, and for any element $b \in \mathbb{Z}_n^*$ let its order be m, we have $b^m = 1$ and since order of element divides order of group, m divides $\phi(n)$, and hence $b^{\phi(n)} = 1$.

1.4.2 Euler's theorem

Euler did a generalisation of Fermat's theorem. If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is divisible by n , i.e $a^{\phi(n)} \equiv 1 \mod n$.

Proof: Suppose $a \equiv b \mod n$, where $0 \leq b \leq n-1$, then $a^{\phi(n)} \equiv b^{\phi(n)} \mod n$ and as a is co-prime to n, and n divides $a - b$, so b must also be co-prime to n thus $b \in \mathbb{Z}_n^*$, thus from above discussion we have $b^{\phi(n)} \equiv 1 \mod n$, hence $a^{\phi(n)} \equiv 1 \mod n$. Hence proved.

2 Orbit-Stabiliser theorem and Burnside's lemma

2.1 Group action on a set, orbits, stabilizer

Consider a group G and a set S. An action of G on S is a mapping * from $G \times S \to S$, such that:

- $e * s = s \quad \forall s \in S$
- $(g_1 g_2) * s = g_1 * (g_2 * s) \quad \forall s \in S$ and $g_1, g_2 \in G$

What are orbits?
Define a relation $\sim$ on S , such that $s \sim t$ if and only if $\exists g \in G$ such that $g * s = t$. This relation turns out to be an equivalence relation. It partitions the set S into equivalence classes called as orbits.

What are stabilisers? For an element s in the set S, the stabilizer of s is the set of elements $g \in G$ such that $g * s = s$. Note that a stabilizer(for any s) is a subgroup of G.

2.2 Example

Consider a triangle in the plane. Each vertex can be coloured either red or blue.
Let S denote all possible configurations. So, $S = \{BBB, BBR, BRB, RBB, BRR, RBR, RRB, RRR\}$.

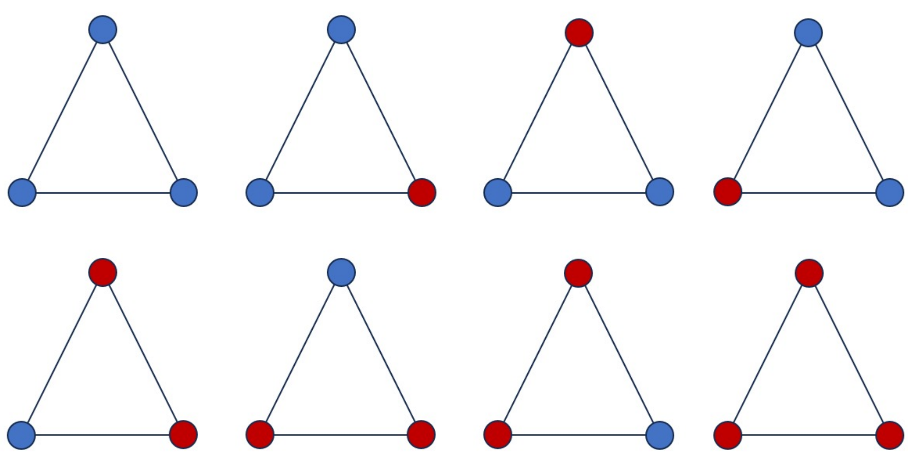

Figure 1: Elements of S

Let $G = \{e, r, r^2\}$ denote the symmetries of triangle, that is identity (e), rotation by $120°(r)$ and rotation by $240°(r^2)$.
Now we let G act on S in the natural way. For example $r(BRR) = RBR, r(BBB) = BBB$.
Simply apply that transformation on the triangle and see the new colouring.

2.3 Orbit-Stabilizer theorem

Let s be any element of set S.
The no.of elements in the orbit of s is equal to the Index of stabilizer of s.

Note: Index of a subgroup H of G is the value $\frac{|G|}{|H|}$, i.e ratio of orders of group and subgroup.

Proof: Let H be the stabilizer of s. So, H is a subgroup of G. Note that $g' * s = g * s \iff g' \in gH$, where gH is the left coset of H containing g. Now, consider the equivalence relation $\sim^*$ such that $g_1 \sim^* g_2 \iff g' * s = g * s$. So, it implies $g_1 \sim^* g_2 \iff g' \in gH$. Hence, no. of equivalence classes under this relation are nothing but no. of left cosets of H, which is $\frac{|G|}{|H|}$ (Index of H). Let Gs be the set $\{g * s | g \in G\}$. No. of distinct elements in Gs is equal to no. of equivalence classes , i.e $\frac{|G|}{|H|}$, and also no. of distinct elements in Gs is nothing but no. of elements in orbit of s. Hence proved.

2.4 Burnside's lemma

Let g be an element of G, define X_g as the set of elements of S fixed by g , i.e $X_g = \{x \in S | g * x = x\}$.
If r is the no. of orbits in S, then

$$r \cdot |G| = \sum_{g \in G} |X_g| \tag{1}$$

2.5 Exercises

1. Prove that example 2.2 is a valid group action.
2. Prove Burnside's lemma. (Hint : Count RHS in a different way)
3. Prove that the relation $\sim$ defined previously as $s \sim t$ if and only if $\exists g \in G$ such that $g * s = t$, is an equivalence relation.