1 Group Actions

Galois: $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_2$

CAYLEY: $|G| = n$ is isomorphic to a subgroup of S_n

Definition 1.1: Group action

G acting on a set X is $\alpha : G \times X \to X$ such that $\alpha(g, h) = \alpha_g(x)$.

Or equivalently, $\alpha : G \to \text{Perm}(X) \cong S_{|x|}$ such that $\alpha(g) = \alpha_g$

The action satisfies:

(1) $\alpha_e(x) = x$

(2) $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$

Notation: the action gives $x \in X \to g \cdot x \in X$

Definition 1.2: Orbits

The subsets of X given by $G \cdot x = \{y \in X \mid y = g \cdot x \text{ for some } g \in G\}$

Notice: Orbits partition G.

Proposition 1.3

The group action is transitive if there is only one orbit.

Transitive: for any $x \in X$, we can find $g \in G, y \in X$ such that $x = g \cdot y$

Proposition 1.4

The group action defines an equivalence relation on X with equivalence classes = orbits

Definition 1.5: Stabilizers

For $x \in X$, stabilizers is the subgroup of G, $G_x = \{g \in G \mid g \cdot x = x\}$.

We say the action is **free** if all stabilizers are trivial (no non-identity elements of G has a fixed point $g \cdot x = x$).

Theorem 1.6: Orbit-Stabilizer Theorem

$|G| = |G_x| \times |G \cdot x|$ = (order of stabilizer of x) × (order of orbit of x).

Proof. (Lagrange's Theorem staff) □

Lemma 1.6.1

The group actions give homomorphism $\alpha : G \to \text{Perm}(X)$

Theorem 1.7: Cayley's Theorem

Every finite group G is (isomorphic to) a subgroup of a symmetric group. Specifically: $|G| = n, G \cong S \leqslant S_n$.

Example 1.8. Groups acting on themselves:

(1) Left multiplication: $m : G \to \text{Perm}(G)$ such that $m_g(x) = mg$. The orbits of this action are left cosets.

(2) Conjugation: $\alpha : G \to \text{Perm}(G)$ which is $G \to \text{Auto}(G)$ actually. $\alpha_g(x) = gxg^{-1} = \underbrace{x^g}_{\text{conjugation notation}}$

For part (2):
Orbits = conjugacy classes

$$Cl(x) = \left\{y \in G \mid y = gxg^{-1} = x^g \text{ for some } g \in G\right\}$$

Stabilizers: centralizers

$$G_x = C_G(x) = \left\{g \in G \mid gxg^{-1} = x\right\} = \{g \in G \mid gx = xg\}$$

Note: If x conjugate to y then $Cl(x) = Cl(y)$

Proposition 1.9

FACT:

(1) $|G| = |C_G(x)| \times |Cl(x)| \implies |Cl(x)| = [G : C_G(x)] \implies |Cl(x)| \mid |G|$ for every x.

(2) Class equation: $G = \sqcup_i Cl(g_i)$, g_i representatives of conjugacy classes. This means

$$|G| = \sum_i |Cl(g_i)| = \sum_i [G : C_G] = |Z(G)| + \underbrace{\sum_{i=k} [G : C_G(x_i)]}_{\text{sum of } |Cl(x)| \neq 1}$$

(3) If $x \in Z(G)$, $|Cl(x)| = 1$

Proposition 1.10: 7.3.1

Center of a p-group is non-trivial. (Note if G is a p-group, $|G| = p^k$ for some integer k.

Proof. $|G| = p^k$. By class equation, $|G| = |Z(G)| + \sum_i [H : C_G(x_i)]$. Suppose $|Z(G)| = 1$, so $p^k = 1 + \sum_i [G : C_G(x_i)]$. And $[G : C_G(x_i)] \mid p^k \implies = p^{m_i}$. So

$$\begin{aligned} p^k &= 1 + \sum_{i=1}^{k} p^{m_i} \\ &= 1 + p(p^{m_1 - 1} + p^{m_2 - 1} + \ldots + p^{m_k - 1}) \\ &\equiv 1 (\text{mod } p) \end{aligned}$$

Contradiction. So $|Z(G)| \neq 1$. □

Proposition 1.11: 7.3.3

Groups of order p^2 are abelian.

Proof. $|G| = p^2$, we want to show $|Z(G)| = p^2$. By previous proposition, $|Z(G)| \neq 1$, so $|Z(G)| = p$ or p^2. We want to rule out the possibility of order being p. $|G| = |Z(G)| + \sum_{i=1}^{k}[G : C_G(x_i)]$. Notice the order cannot exceed p^2, the nontrivial conjugacy classes should have order p. Note that if $x \notin Z(G)$, then $Z(G) < C_G(x) \implies |C_G(x)| = p^2$, which is a contradiction. □

1.1 Dihedral Groups

Definition 1.12: Dihedral Group

Groups of symmetries of regular n-gons $= \{n$ rotations, n reflection$\}$
Notation: D_n (in book) or D_{2n} (modern notation).
We have

$$D_{2n} = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle$$

Another general rule: compose two reflection, get the rotation corresponding $2 \times \theta$ where θ = angle between the axes of rotations.

Proposition 1.13

n odd:

- $Z(D_{2n}) = \{e\}$
- All reflections are conjugate (they are all in the same conjugacy class)

n even:

- $Z(D_{2n}) = \{e, r^{\frac{n}{2}}\}$
- Vertex axis reflections are conjugate, fare axis reflections are conjugate. That is, there are two conjugacy classes: vertex axis reflections and fare axis reflections

Example 1.14. Class equation for $D_8 = \{$symmetries of square$\}$
We can think about the elements of D_8 as the elements of S_4 because each element permutes the vertices:

$$r \to (1234)$$
$$s_1 \to (23)$$
$$s_2 \to (12)(34)$$

(1) $Z(D_8) = \{e, (13)(24)\} = \{e, r^2 \equiv S_1 S_3\}$

(2) $Cl((13)) = \{(13), (24)\}$ (vertex axis reflections)
$Cl((12)(34)) = \{(12)(34), (14)(23)\}$ (fare axis reflections)

$Cl(r) = Cl((1234)) = \{(1234)(1432)\}$ (order 4 rotations)

Homework hint (problem 10): Classify group of order 8 =

$$(1) \quad 3 \text{ abelian } = \begin{cases} \mathbb{Z}/8\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases}$$

$$(2) \quad 2 \text{ non-abelian } = \begin{cases} D_8 \\ Q_8 = \{1, i, j, k, -1, -i, -j, -k\} \end{cases}$$

1.2 Simple groups

Definition 1.15: Simple groups

Simple groups have no non-trivial normal subgroups. The simple groups are the building blocks of all groups (Some side reading: classification of simple groups)

Lemma 1.15.1: 7.4.2

For normal subgroup $N \trianglelefteq G$ ($gNg^{-1} = N$), we have

(1) $x \in N \implies Cl(x) \subseteq N$

(2) $N = \bigcup_x Cl(x)$

(3) $|N| = \sum_{x \text{ represents of distinct conjugacy class}} |Cl(x)|$

Theorem 1.16: 7.4.3

A_5 is simple where A_5 = icosahedral group = even parts of permutation in S_5

Proof. We've given that A_5 has the following class equation:

$$|A_5| = 60 = 1 + 20 + 12 + 12 + 15$$

which is established with geometry in book section 7.4.
Suppose N is normal in A_5, then $|N| \mid 60$. By proposition (3) in the lemma, $|N| = 1 + m$ where m = sum of subset of $\{20, 12, 12, 15\}$. But no such integer m with these combined property $\implies$ no normal subgroup. □

The theorem of **Galois group** (we don't need to know for now): Galois group of polynomial $\Leftrightarrow$ polynomial is solvable by radicals. We have $Gal(\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_5)/\mathbb{Q}) \leqslant A_5$. Since A_5 is not solvable, degree 5 polynomials are not solvable by radicals (has no formula of roots in terms of n)

1.3 Conjugacy classes in S_n

Example 1.17. We can think about S_5 as $\phi : \{1,2,3,4,5\} \to \{a,b,c,d,e\}$. Consider $p \in S_n$, $\phi \circ p \circ \phi^{-1} : \{a,b,c,d,e\} \to \{a,b,c,d,e\}$. Let $q = (1452), p = (134)(25)$. We have

$$qpq^{-1} = (1452)(134)(25)(2541) = (435)(12) = p'$$

We find that p and its conjugate p' have same disjoint cycle decomposition (cycle structure). And we find that $\phi : \{1,2,3,4,5\} \to \{4,1,3,5,2\}$ maps p to p', which is exactly the same as q.

Proposition 1.18: 7.5.1

p and p' are conjugate in Sn $\Leftrightarrow$ cycle decompositions are the same length (see the example above).

Example 1.19. Consider class equation for S_4:

Conjugacy classes	partition of 4	#
e	1+1+1+1	1
(**)	1+1+2	6
(**)(**)	2+2	3
(***)	1+3	8
(****)	4	6

Table 1

Group of order 8 (Problem 10): If abelian, $= 1+1+1+1+1+1+1+1$. If not, $= 1+1+2+2+2$

Example for abelian case: Let $|G| = p^2q^2$, the possible groups are $\mathbb{Z}/p^2q^2\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q^2\mathbb{Z}, \ldots$ ($p \times p \times q^2, p^2 \times q \times q, p \times p \times q \times q$ of the same form)

Now let's see $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. We know $(-1)^2 = 1, i^2 = j^2 = k^2 = -1, ijk = -1$. And $Z(Q_8) = \{\pm 1\}$.

<u>Class equation for Q_8:</u> Recall $|Cl(x)| = [Q_8 : C_G(x)]$, and $C_G(i) = \{x \in Q_8 \mid xi = ix\} = \{1, i, -1, -i\}$. Similarly $C_G(j) = \{1,-1,j,-j\}, C_G(k) = \{1,-1,k,-k\}$. So $[Q_8 : C_G(x)] = 2$ for all $x = i, j, k$.

To distinguish D_8 and Q_8, see what their normal subgroups are.