20250211 MATH3301 NOTE 10[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Group Action

1.1 Category Axioms

Definition 1.1. (**Group Action**)
Let G be a group, X be a set, and $*: G \times X \to X$ be a map. If:

$$\forall x \in X, e * x = x$$
$$\forall g, h \in G \text{ and } x \in X, (gh) * x = g * (h * x)$$

Then G acts on X via $*$.

Proposition 1.2. Let G be a group, X be a set, and $*: G \times X \to X$ be a map. G acts on X via $*$ iff $\sigma : G \to \mathrm{Perm}(X), g \mapsto \ell_g$ is a group homomorphism.

Proof. We may divide our proof into two parts.
"if" direction: Assume that $\sigma : G \mapsto \mathrm{Perm}(X), g \mapsto \ell_g$ is a group homomorphism.

$$\forall x \in X, e * X = \ell_e(x) = x$$
$$\forall g, h \in G \text{ and } x \in X, (gh) * x = \ell_{gh}(x) = \ell_g(\ell_h(x)) = g * (h * x)$$

"only if" direction: Assume that G acts on X via $*$.

$$\forall g \in G, \ell_g^{-1} = \ell_{g^{-1}} \implies \ell_g \in \mathrm{Perm}(X)$$
$$\forall g, h \in G \text{ and } x \in X, \ell_{gh}(x) = (gh) * x = g * (h * x) = \ell_g(\ell_h(x)) \implies \ell_{gh} = \ell_g \ell_h$$

Quod. Erat. Demonstrandum. □

Definition 1.3. (**Group Action Homomorphism**)
Let G be a group acting on X, X' via $*, *'$, and $\sigma : X \to X'$ be a map. If:

$$\forall g \in G \text{ and } x \in X, \sigma(g * x) = g *' \sigma(x)$$

Then σ is a group action homomorphism.

Proposition 1.4. Let G be a group acting on X, X' via $*, *'$.
If $\sigma : X \to X'$ is a group action homomorphism, then:
(1) If $*'$ can be restricted to $Y' \subseteq X'$, then $*$ can be restricted to $\sigma^{-1}(Y') \subseteq X$.
(2) If $*$ can be restricted to $Y \subseteq X$, then $*'$ can be restricted to $\sigma(Y) \subseteq X'$.

Proof. We may divide our proof into two parts.
Part 1: Assume that $*'$ can be restricted to $Y' \subseteq X'$.

$$\sigma(G * \sigma^{-1}(Y')) = G *' \sigma(\sigma^{-1}(Y')) \subseteq G *' Y' \subseteq Y' \implies G * \sigma^{-1}(Y') \subseteq \sigma^{-1}(Y')$$

Part 2: Assume that $*$ can be restricted to $Y \subseteq X$.

$$G * Y \subseteq Y \implies G *' \sigma(Y) = \sigma(G * Y) \subseteq \sigma(Y)$$

Quod. Erat. Demonstrandum. □

Proposition 1.5. Let G be a group acting on X, X' via $*, *'$.
If $\sigma : X \to X'$ is a bijective group action homomorphism, then so is σ^{-1}.

Proof. As σ is bijective, so is σ^{-1}. In addition, for all $g \in G$ and $x' \in X'$:

$$\sigma^{-1}(g *' x') = \sigma^{-1}(g *' \sigma(\sigma^{-1}(x'))) = \sigma^{-1}(\sigma(g * \sigma^{-1}(x'))) = g * \sigma^{-1}(x')$$

Quod. Erat. Demonstrandum. □

1.2 Orbit Space and Burnside's Lemma

Definition 1.6. (**Orbit Space**)
Let G be a group acting on X via $*$. For all $x \in X$, define the orbit of x as $G * x$.
Define the orbit space X/G of X as the collection of all orbits.

Example 1.7. $\mathbb{Z}$ acts on $\mathbb{Z}$ transitively by translation, and $\mathbb{Z}$ trivially acts on $\{\mathrm{i}\}$ by fixing it. If we union them, then the orbits $\mathbb{Z}, \{\mathrm{i}\}$ have distinct cardinalities.

Proposition 1.8. Let G be a group acting on X via $*$. X/G partitions G.

Proof. It suffices to prove that $x \sim g * x$ is an equivalence relation on X.
Part 1: $x \sim e * x = x$.
Part 2: $x \sim g * x \implies g * x \sim g^{-1} * (g * x) = (g^{-1}g) * x = e * x = x$.
Part 3: $x \sim h * x$ and $h * x \sim g * (h * x) \implies x \sim (gh) * x = g * (h * x)$.
Quod. Erat. Demonstrandum. □

Example 1.9. Let G be a group acting on X via $*$ such that X/G is finite.

$$|X/G| = \sum_{\mathrm{Orb} \in X/G} 1 = \sum_{\mathrm{Orb} \in X/G} \frac{\sum_{x \in \mathrm{Orb}} 1}{\sum_{x \in \mathrm{Orb}} 1} = \sum_{\mathrm{Orb} \in X/G} \sum_{x \in \mathrm{Orb}} \frac{1}{|G * x|} = \sum_{x \in X} \frac{1}{|G * x|}$$

Definition 1.10. (**Stabilizer**)
Let G be a group acting on X via $*$. For all $x \in X$, define the stabilizer of x as:

$$G_x = \{g \in G : g * x = x\}$$

Proposition 1.11. Let G be a group acting on X via $*$.

$$\forall x \in X, G_x \leq G$$

Proof. For all $x \in X$:
Part 1: $e * x = x \implies e \in G_x$.
Part 2: $g, h \in G_x \implies (gh) * x = g * (h * x) = g * x = x \implies gh \in G_x$.
Part 3: $g \in G_x \implies g^{-1} * x = g^{-1} * (g * x) = (g^{-1} g) * x = e * x = x \implies g^{-1} \in G_x$.
Quod. Erat. Demonstrandum. $\square$

Example 1.12. $G = A_5$ act on $X = \{1, 2, 3, 4, 5\}$ via evaluation.
As A_5 is simple, $G_1 \cong A_4$ is not normal in G, so G/G_1 is not a group.

Proposition 1.13. Let G be a group acting on X via $*$.
For all $x \in X$, the following map is a bijection:

$$\sigma : G/G_x \to G * x, gG_x \mapsto g * x$$

Proof. σ is clearly surjective. We show that σ a well-defined injection:

$$gG_x = hG_x \iff g \in hG_x \iff g * x = h * x$$

Quod. Erat. Demonstrandum. $\square$

Definition 1.14. (**Fixed Set**)
Let G be a group acting on X via $*$. For all $g \in G$, define the fixed set of g as:

$$X_g = \{x \in X : g * x = x\}$$

Example 1.15. (**Burnside's Lemma**)
Let G be a group acting on X via $*$.
If $\textbf{Fix} = \{(g, x) \in G \times X : g * x = x\}$ is finite, then:

$$\sum_{g \in G} |X_g| = |\textbf{Fix}| = \sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|G/G_x|} = |G| \sum_{x \in X} \frac{1}{|G * x|} = |G||X/G|$$

Example 1.16. Assume that $G = D_p$ is the dihedral group of a regular p-gon, where $p \geq 3$ is a prime number, X be the collection of all m-color edge coloring approaches of a regular p-gon, and $*$ be the evaluation action of G on X.

$$|X/G| = \frac{m^p + \sum_{g \in \mathbb{Z}_p^\times} m + \sum_{g \in \sigma \mathbb{Z}_p} m^{\frac{p+1}{2}}}{1 + (p-1) + p} = \frac{m^p + (p-1)m + pm^{\frac{p+1}{2}}}{2p}$$

1.3 Class Equation and Sylow's Theorems

Proposition 1.17. Let G be a group acting on X via $*$.

$$\forall x, y \in X, G * x = G * y \implies G_x, G_y \text{ are conjugate}$$

Proof. For all $x, y \in X$:

$$(gG_xg^{-1}) * y = (gG_xg^{-1}) * (g * x) = g * x = y \implies gG_xg^{-1} \subseteq G_y$$
$$(g^{-1}G_yg) * x = (g^{-1}G_yg) * (g^{-1} * y) = g^{-1} * y = x \implies g^{-1}G_yg \subseteq G_x$$

Quod. Erat. Demonstrandum. □

Example 1.18. (**Orbit Decomposition**)
Let G be a group acting on X via $*$. If X is finite, then:

$$\begin{aligned} |X| &= \sum_{G*x \in X/G} |G * x| = |X_G| + \sum_{|G*x|>1} |G * x| \\ &= |X_G| + \sum_{|G/G_x|>1} |G/G_x| = |X_G| + \sum_{G_x \lneq G} \frac{|G|}{|G_x|} \end{aligned}$$

Here, $X_G = \bigcap_{g \in G} X_g$.

Example 1.19. (**Class Equation**)
Let G be a group, and N be a normal subgroup of G.
G acts on N by conjugation with $N_G = N \cap Z_G$, so:

$$|N| = |N \cap Z_G| + \sum_{|G*n|>1} |G * n|$$

Definition 1.20. (**p-group**)
Let G be a group, and p be a prime number.
If for some $n \geq 0$, $|G| = p^n$, then G is a p-group.

Proposition 1.21. Let G be a group, and p be a prime number.
If G is a nontrivial p-group, then $|Z_G|$ is a nontrivial multiple of p.

Proof. Take the normal subgroup G of G, and consider the class equation:

$$|G| = |Z_G| + \sum_{|G*n|>1} |G * n|$$

As G is a nontrivial p-group, for some $n \geq 1$, $|G| = p^n$.

Hence, all nontrivial factors of G are divisible by p, which implies:

$$p \text{ divides } |G| - \sum_{|G*n|>1} |G*n| = |Z_G|$$

As $Z_G \ni e$ is nonempty, $|Z_G|$ is a nontrivial multiple of p.
Quod. Erat. Demonstrandum. $\square$

Definition 1.22. (**p-Sylow Subgroup**)
Let G be a finite group, p be a prime number, and P be a subgroup of G.
If P is a p-group with maximal p-multiplicity, then P is p-Sylow.

Example 1.23. Every prime number p induces a strict total order $<_p$ on $\mathbb{N}$:
(1) If the p-multiplicity of l is less then that of l', then $l <_p l'$.
(2) If the p-multiplicity of l is equal to that of l' and $l < l'$, then $l <_p l'$.

Theorem 1.24. (**Sylow's First Theorem**)
Let G be a finite group, and p be a prime number.
The set $\mathbf{P}_G$ of all p-Sylow subgroups of G is nonempty.

Proof. We apply the strong form of mathematical induction.
Part 1: When $|G| <_p p$, $\mathbf{P}_G = \{\{e\}\}$ is nonempty.
Part 2: When for some $n \geq 0$, $|G| = p^n$, $\mathbf{P}_G = \{G\}$ is nonempty.
Part 3: For all $n \geq 1$, we wish to show the following implication:

$$\text{The theorem holds when } |G| <_p p^n \implies \text{The theorem holds when } |G| <_p p^{n+1}$$

As the theorem is true when $|G| \leq_p p^n$, it suffices to consider the case $p^n <_p |G| <_p p^{n+1}$.
Case 3.1: If some proper stabilizer subgroup G_x of G has order $|G_x| \geq_p p^n$, then:
(1) Replace G by G_x and repeat the algorithm, until no such G_x is found.
(2) If $|G|$ is reduced to a power of p, then go to **Part 2**.
(3) If $|G|$ is not reduced to a power of p, then go to **Case 3.2**.
Case 3.2: If no proper stabilizer subgroup G_x of G has order $|G_x| \geq_p p^n$, then:
(1) From class equation and Cauchy's theorem, Z_G contains an element ξ of order p.
(2) ξ generates a normal subgroup $\langle \xi \rangle$ of G, and $|G/\langle \xi \rangle| = |G|/p <_p p^{n+1}/p = p^n$.
(3) From inductive hypothesis, $\mathbf{P}_{\widetilde{G}}$ is nonempty, where $\widetilde{G} = G/\langle \xi \rangle$.
(4) From the first isomorphism theorem, $\mathbf{P}_G \supseteq \pi^{-1}(\mathbf{P}_{\widetilde{G}})$ is nonempty, where $\pi : g \mapsto \widetilde{g}$.
Quod. Erat. Demonstrandum. $\square$

Theorem 1.25. (**General Cauchy's Theorem**)
Let G be a finite group, and p be a prime number.
If p divides $|G|$, then G has an element ξ of order p.

Proof.

$$\begin{aligned} p \text{ divides } |G| &\implies G \text{ has a nontrivial } p\text{-Sylow subgroup } P \\ &\implies |Z_P| \text{ is a nontrivial multiple of } p \\ &\implies Z_P \text{ has an element } \xi \text{ of order } p \end{aligned}$$

Quod. Erat. Demonstrandum. $\square$

Lemma 1.26. Let G be a nontrivial p-group acting on a finite set X, whose cardinality $|X|$ is not divisible by p. $X_G \neq \emptyset$.

Proof. According to orbit decomposition formula:

$$|X| - |X_G| \equiv \sum_{G_x \lneq G} \frac{|G|}{|G_x|} \equiv \sum_{G_x \lneq G} \text{Nontrivial Factor of } p^n \equiv 0 (\text{mod } p)$$

As $|X|$ is not divisible by p, so does $|X_G|$, which implies $X_G \neq \emptyset$.
Quod. Erat. Demonstrandum. $\square$

Lemma 1.27. Let G be a group, and H, Q be subgroups of G.
If H acts on Q by conjugation, then:
(1) HQ is a subgroup of G.
(1) Q is normal in HQ.
(2) $H \cap Q$ is normal in H.
(3) $H/(H \cap Q), (HQ)/Q$ are isomorphic.

Proof. We may divide our proof into four parts.
Part 1: $HQ = QH \implies HQ \leq G$.
Part 2: $(h'q')q(h'q')^{-1} = h'(q'qq'^{-1})h'^{-1} \in Q \implies Q$ is normal in HQ.
Part 3: $hqh^{-1} \in H \cap Q \implies H \cap Q$ is normal in H.
Part 4: From the second isomorphism theorem, $H/(H \cap Q), (HQ)/Q$ are isomorphic.
Quod. Erat. Demonstrandum. $\square$

Theorem 1.28. (**Sylow's Second Theorem**)
Let G be a finite group, p be a prime number, and P be a p-Sylow subgroup of G. The G-conjugates of P cover all p-subgroup H of G.

Proof. We may divide our proof into two steps.
Step 1: We construct a special conjugate Q of P.
(1) As $H \leq G$, the p-group H acts on all G-conjugates $G * P$ of P by conjugation.
(2) As P is p-Sylow, $|G * P| = |G|/|G_P| = \frac{|G|/|P|}{|G_P|/|P|}$, so $|G * P|$ is not divisible by p.
(3) Hence, some G-conjugate Q of P is fixed under H-conjugation.
Step 2: We prove that H is contained in this conjugate Q of P.

(1) As H acts on Q by conjugation, $H/(H \cap Q), (HQ)/Q$ are isomorphic.
(2) As Q is p-Sylow, $HQ = Q$, so $H = H \cap Q$, which implies $H \subseteq Q$.
Quod. Erat. Demonstrandum. □

Example 1.29. Let G be a finite group, and p be a prime number.
G acts on $\mathbf{P}_G$ transitively by conjugation $*$, so $|\mathbf{P}_G| = |G * P|$ divides $|G|$.

Theorem 1.30. (**Sylow's Third Theorem**)
Let G be a finite group, and p be a prime number.
If we restrict $*$ to a p-Sylow subgroup Q of G, then $(\mathbf{P}_G)_Q = \{Q\}$.

Proof. It is clear that $\{Q\} \subseteq (\mathbf{P}_G)_Q$.
For all $H \in (\mathbf{P}_G)_Q$, $H/(H \cap Q), (HQ)/Q$ are isomorphic.
As H, Q are p-Sylow, $HQ = Q$, so $H = H \cap Q = Q \in \{Q\}$.
Quod. Erat. Demonstrandum. □

References

[1] H. Ren, “Template for math notes,” 2021.