NOTES ON GROUP THEORY

SHENGXI JIN

1. CATEGORY CONSTRUCTIONS

Definition 1.1. Suppose we have a category $\mathcal{C}$. An object G in $\mathcal{C}$ is called a group object if it is endowed with morphisms $m\colon G\times G\to G$, $i\colon G\to G$ and $e\colon \{*\}\to G$ corresponding to multiplication, inversion, and an identity section. Here, the product is the product in $\mathcal{C}$ and $\{*\}$ denotes the final object. We require these morphisms to satisfy commutative diagrams:

- Associativity:

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mathrm{id}\times m} & G\times G \\ \downarrow{\scriptstyle m\times\mathrm{id}} & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\quad m\quad} & G \end{array}$$

- Identity:

$$\begin{array}{ccccc} & & \{*\}\times G & \xrightarrow{e\times\mathrm{id}} & G\times G \\ & \nearrow & & & \searrow{\scriptstyle m} \\ G & & \xrightarrow{\quad\mathrm{id}\quad} & & G \\ & \searrow & & & \nearrow{\scriptstyle m} \\ & & G\times\{*\} & \xrightarrow{\mathrm{id}\times e} & G\times G \end{array}$$

- Inverse:

$$\begin{array}{ccccc} & & G\times G & & \\ & \nearrow{\scriptstyle i\times\mathrm{id}} & & \searrow{\scriptstyle m} & \\ G & \longrightarrow & \{*\} & \xrightarrow{e} & G \\ & \searrow{\scriptstyle \mathrm{id}\times i} & & \nearrow{\scriptstyle m} & \\ & & G\times G & & \end{array}$$

Definition 1.2. Suppose $\mathcal{C}$ is a category and G, H are objects in $\mathcal{C}$. Homomorphisms of G, H are their morphisms in $\mathcal{C}$.

If we take $\mathcal{C} = \mathbf{Set}$, definition of group object and homomorphism would simply be tatutology of the usual group axioms and the usual group homomorphism. However, it indeed tells us how to consider objects analogous to groups, which are built on more complicated structures than sets. For example, for $\mathcal{C} = \mathbf{Top}, \mathbf{Man}^{\infty}, S\text{-}\mathbf{Sch}$, group objects are topological groups, Lie groups and group schemes over base scheme S respctively while homomorphisms are group homomorphisms preserving additional structures.

We shall still consider the usual groups in the remainder of this article.

Definition 1.3. Suppose

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \longrightarrow G_n \xrightarrow{f_n} \cdots$$

is a sequence of group homomorphisms. This sequence is said to be exact if $\operatorname{Ker} f_{i+1} = \operatorname{Im} f_i$. It is conventional to denote the trivial group by 0 in exact sequences.

Exact sequence is a common and fundamental language in modern algebra.

Example 1.4. For a group homomorphism $f\colon G\to H$, we have:

(1) f is injective if and only if $0 \longrightarrow G \xrightarrow{f} H$.
(2) f is surjective if and only if $G \xrightarrow{f} H \longrightarrow 0$.
(3) f is isomorphism if and only if $0 \longrightarrow G \xrightarrow{f} H \longrightarrow 0$.

Example 1.5. Let $0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$ be an exact sequence. If $H = \operatorname{Ker} g$ we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \end{array}$$

in which the vertical maps are isomorphisms. The first and the second rows are isomorphisms, so it can be shown that so is the third row. Hence the exact sequence is equivalent to say

$$\operatorname{Im} g \simeq G/\operatorname{Ker} f$$

Now we investigate a more concrete but also more complicated example arising from topology. Many details may be omitted in view of space limitations.

Example 1.6 (homotopy group and relative homotopy group)**.** Let X be a topological space. Choose base points $x_0 \in X$ and $p \in S^n$. The homotopy classes of continuous maps $(S^n, p) \to (X, x_0)$ forms the n-th homotopy group $\pi_n(X, x_0)$ of X. For $n = 0$, $\pi_n(X, x_0)$ is simply the set of path-components of X. For $n = 1$, $\pi_n(X, x_0)$ is the fundamental group of X.

Let $A \subset X$ be a subspace containing x_0. We can consider a very useful generalization of the homotopy groups, the relative homotopy groups $\pi_n(X, A, x_0)$. Homotopy theory says that there is a long excat sequence

$$\begin{aligned} \cdots \longrightarrow \pi_n(A, x_0) \xrightarrow{i_*} \pi_n(X, x_0) \xrightarrow{j_*} \pi_n(X, A, x_0) \xrightarrow{\partial} \pi_{n-1}(A, X_0) \longrightarrow \cdots \\ \longrightarrow \pi_0(A, x_0) \longrightarrow \pi_0(X, A, x_0) \longrightarrow \pi_0(X, x_0) \end{aligned}$$

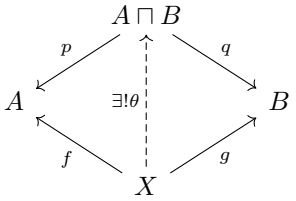
Near the end of the sequence, where group structures are not defined, exactness still makes sense: The image of one map is the kernel of the next, those elements mapping to the homotopy class of the constant map.

Suppose $p\colon E \to B$ is a fiber bundle with the homotopy lifting property with respect to every D^k. Choose base points $b_0 \in B$ and $x_0 \in F = p^{-1}(b_0)$ and then $p_*\colon \pi_n(E, F, x) \to \pi_n(B, b_0)$ would be an isomorphism for $n \geqslant 1$. Hence if B is path-connected, there is a long exact sequence

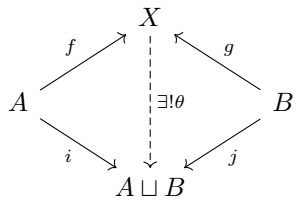
$$\begin{aligned} \cdots \longrightarrow \pi_n(F, x_0) \xrightarrow{i_*} \pi_n(E, x_0) \xrightarrow{p_*} \pi_n(B, b_0) \longrightarrow \pi_{n-1}(F, X_0) \longrightarrow \cdots \\ \longrightarrow \pi_0(F, x_0) \longrightarrow \pi_0(E, x_0) \longrightarrow \pi_0(B, b_0) \end{aligned}$$

The nicest example would probably be the famous Hopf fibration $S^1 \to S^3 \to S^2$. Further discussions in homotopy theory will show that $\pi_n(S^n) = \mathbb{Z}$, $\pi_n(S^1) = 0$ for all $n \geqslant 1$ and $\pi_2(S^3) = \pi_1(S^3) = 0$, so we get $\pi_n(S^3) = \pi_n(S^2)$ for $n \geqslant 3$. In particular, $\pi_3(S^2) = \pi_3(S^3) = \mathbb{Z}$. We see that $\pi_n(S^m)$ can be non-trivial when $n > m$, which is different from homology groups.

Definition 1.7. Let A, B be objects in category $\mathcal{C}$. The product of A, B is a triple $(A \sqcap B, p, q)$ where $A \sqcap B$ is an object in $\mathcal{C}$ and $p\colon A \sqcap B \to A$, $q\colon A \sqcap B \to B$ are morphisms, called projections, such that for every object X and every pair of morphisms $f\colon X \to A$ and $g\colon X \to B$, there exists a unique morphism $\theta\colon X \to A \sqcap B$ such that



Similarly, the product of A, B is a triple $(A \sqcup B, i, j)$ where $A \sqcup B$ is an object in $\mathcal{C}$ and $i\colon A \to A \sqcup B$, $j\colon B \to A \sqcup B$ are morphisms, called injections, such that for every object X and every pair of morphisms $f\colon A \to X$ and $g\colon B \to X$, there exists a unique morphism $\theta\colon A \sqcup B \to X$ such that



It is not true that products and coproducts always exist, but in many familiar categories they do, including **Grp**. Also, we can show that if products and coproducts exist they are unique up to an isomorphism.

Definition 1.8. Let G, H be groups. Suppose $\langle S_G \mid R_G \rangle, \langle S_G \mid R_G \rangle$ are presentations of G, H respectively,

2. group action and Sylow theorems

In this section, we always assume G to be a group and X to be a (nonempty) set.

Definition 2.1 (group action)**.** A group action on X is a group homomorphism

$$\rho\colon G \longrightarrow \mathrm{Sym}(X)$$

Notation $G \curvearrowright X$ indicates that G admits an action on X. If $g \in G$ and $x \in X$, we usually denote $\rho(g)x$ by gx for convenience.

Proposition 2.2. Suppose $G \curvearrowright X$, then
(1) $1x = x, \forall x \in X$.
(2) $(gh)x = g(hx), \forall x \in X, g, h \in G$.
conversely, given a map $\phi\colon G \times X \to X$ satisfying the above propoty, we can reconstruct the group action ρ.

Definition 2.3. Suppose $G \curvearrowright X$. There is an equivalence relation on X defined by $x \sim y \Leftrightarrow \exists g \in G, y = gx$. The equivalence class of x is called the orbit of x and is usually denoted by Gx. Then we have the orbit partition

$$X = \bigsqcup_{x \in X} Gx$$

For every$S \subset X$, it can be checked that the set $\{\, g \in G \mid gS = S \,\}$ forms a subgroup of G. It is called the stabilizar of S, denoted by $\mathrm{Stab}(S)$. In general, $\mathrm{Stab}(S)$ does not need to be normal.

There are three common terminologies to describe group actions with certain propoties.

Definition 2.4. Suppose $G \curvearrowright X$. The action is said to be faithful if ρ is injective; It is said to be free if $\mathrm{Stab}(x) = 1$ for every $x \in X$; It is said to be transitive if the orbit partition is trivial (i.e. $Gx = X$ for some $x \in X$).

There are some basic examples of group actions.

Example 2.5. Every subgroup H of G acts faithfully on G by left translation. The orbit of $g \in G$ is Hg, called the right coset of H. In particualr, the orbit partition of G is a tautology of Lagrange theorem:

$$G = \bigsqcup_{g \in G} Hg$$

Also note that if $H = G$, we get Caylay theorem: $\rho\colon G \to \mathrm{Sym}(G)$ is an injective homomorphism.

Example 2.6. Every subgroup H of G acts transitively on the set of left cosets G/H by left translation with $H = \mathrm{Stab}(H)$.

Example 2.7. G acts on itself by conjugation. For every $x \in G$, the orbit x is called the conjugacy classes; the stabilizer of x is called the the centralizer $C_G(x)$ of x in G. If $H \leqslant G$, the stabilizer of H is called the normalizer $N_G(H)$ of H in G.

It's obvious that $\bigcap_{x \in G} C_G(x)$ is the center of G and $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

Proposition 2.8. Suppose $G \curvearrowright X$, then for every $x \in X$ we have bijection

$$\begin{aligned} G/\operatorname{Stab}(x) &\longrightarrow Gx \\ g\operatorname{Stab}(x) &\longmapsto gx \end{aligned}$$

Corollary 2.9 (counting formula)**.** $|\operatorname{Stab}(x)| \cdot |Gx| = |G|$

The concept of group action provides a significant mindset to approach Sylow theorems.

Definition 2.10 (double coset)**.** Let H and K be subgroups of a group G. A double coset of H and K in G is a set of the form HaK for some $a \in G$.

Proposition 2.11. (double counting formula) Suppose H and K be subgroups of a group G, consider the group action of $H \times K$ on G by $(h,k)g = hgk^{-1}$. The double cosets are orbits and $H \cap aKa^{-1}$ is the stabilizar of $a \in G$. In particular we have

$$|HaK| = \frac{|H||K|}{|H \cap aKa^{-1}|}$$

It gives the double counting formula

$$|G| = \sum_a \frac{|H||K|}{H \cap aKa^{-1}}$$

where the sum is over a set of representatives for the double cosets.

Lemma 2.12. Suppose G is finite. Let p be prime and P be a Sylow p-subgroup of G. For any subgroup H of G, there exists an $a \in G$ such that $H \cap aPa^{-1}$ is a Sylow p-subgroup of H.

Proof. By double counting formula,

$$|G| = \sum_a \frac{|H||P|}{|H \cap aPa^{-1}|}$$

On dividing by |P| we find that

$$\frac{|G|}{|P|} = \sum_a \frac{|H|}{|H \cap aPa^{-1}|}$$

so there exists an a such that $[H : H \cap aPa^{-1}]$ is not divisible by p. For such an a, $H \cap aPa^{-1}$ is a Sylow p-subgroup of H. □

Theorem 2.13 (Sylow I)**.** Let $|G| = n < \infty$, and let p be prime. If p divides n, then G has a Sylow p-subgroup.

Proof. We assume that $n = p^r m$ with m not divisible by p. According to Caylay theorem, G embeds into S_n. S_n also has a faithful action on the basis of $\mathbb{F}_p^n$, which induces $S_n \hookrightarrow \mathrm{GL}(n, \mathbb{F}_p)$ (permutation representation of S_n). By Lemma 2.12 if $\mathrm{GL}(n, \mathbb{F}_p)$ has a Sylow p-subgroup, then so does G.

The $n \times n$ matrices in $\mathrm{GL}(n, \mathbb{F}_p)$ are precisely those whose columns form a basis for $\mathbb{F}_p^n$. Thus, the first column can be any nonzero vector in $\mathbb{F}_p^n$, of which there are $p^n - 1$; the second column can be any vector not in the span of the first column, of which there are $p^n - p$; and so on. Therefore the order of $\mathrm{GL}(n, \mathbb{F}_p)$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$, and so the power of p dividing $|\mathrm{GL}(n, \mathbb{F}_p)|$ is $p^{\frac{1}{2}n(n-1)}$. Consider the upper triangular matrices with the diagonal filled with 1. They happens to form a Sylow p-subgroup of $\mathrm{GL}(n, \mathbb{F}_p)$. □

Corollary 2.14. Suppose G is finite and p is prime. If p^r divides $|G|$ then G admits a subgroup of order p^r.

Proof. Suppose $|G| = n$ and we induction on n. □

Theorem 2.15 (Sylow II)**.** Let p be prime and $|G| = p^r m$ with m not divisible by p.
(a) Any two Sylow p-subgroups are conjugate.
(b) Every p-subgroup of G is contained in a Sylow p-subgroup.
(c) Let s_p be the number of Sylow p-subgroups in G; then $s_p \equiv 1 \mod p$ and $s_p | m$.

Proof. Let P be a Sylow p-subgroup of G, and let P' be a p-subgroup of G. Then P' is the unique Sylow p-subgroup of P', and so Lemma 2.12 with $H = P'$ shows that $P' \subset aPa^{-1}$ for some $a \in G$. This implies (a) and (b).

As for (c), let S be the set of Sylow p-subgroups in G. Take $P \in S$ and let P act on S by conjugation. Notice that $Q \in S$ forms a one-point orbit if and only if $P \subset N_G(Q)$. If $P \subset N_G(Q)$, PQ is a subgroup and $P/(P \cap Q) \simeq PQ/Q$. Since Q is Sylow p-subgroup and $|PQ| = |PQ/Q||Q|$, $|PQ/Q|$ is not divisible by p, which implies $P = Q$. Hence the number of elements in every orbit other than $\{ P \}$ is divisible by p, and we have that $s_p \equiv 1 \mod p$.

By (a) and counting formula, we have

$$s_p = \frac{|G|}{|N_G(P)|} = \frac{|G|}{|P|} \frac{1}{|N_G(P)/P|} = \frac{m}{|N_G(P)/P|}$$

□

3. automorphism and extension

Given a group G, determining $\mathrm{Aut}(G)$ will be a basic question.

Definition 3.1 (inner automorphism and outer automorphism)**.** For $g \in G$, the map

$$\begin{aligned} i_g \colon G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

is an automorphism of G. Automorphisms of this form is called an inner automorphism and the remaining automorphisms are called outer automorphsims.

We have group homomorphism

$$\begin{aligned} G &\longrightarrow G \\ g &\longmapsto i_g \end{aligned}$$

The image, denoted by $\mathrm{Inn}(G)$, is the group of inner automorphisms. Its kernel is the center of G, $Z(G)$, so we get

$$G/Z(G) \simeq \mathrm{Inn}(G)$$

In fact $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$ since for $\alpha \in \mathrm{Aut}(G)$ and $g \in G$ we have

$$\alpha \circ i_g \circ \alpha^{-1} = i_{\alpha(g)}$$

Definition 3.2 (complete group)**.** G is said to be complete if the homomorphism $G \to \mathrm{Aut}(G)$ is an isomorphism.

Two highly non-trivial examples of complete groups are listed below and the proof is omitted.

Example 3.3. (1) S_n is complete for $n \neq 2, 6$.
(2) Simple noncommutative groups are complete.

If N is a normal subgroup of G, we have a special homomorphism

$$\begin{aligned} \theta \colon G &\longrightarrow \mathrm{Aut}(N) \\ g &\longmapsto i_g|_N \end{aligned}$$

If there exists $Q \leqslant G$ such that the restriction of quotient map $\pi|_Q$ is an isomorphism, we can actually reconstruct G from N, Q and $\theta|_Q$.

First notice that $g \in G$ can be written uniquely in the form

$$g = nq, n \in N, q \in Q$$

Then we have a correspondence between G and $N \times Q$. If $g = nq$ and $g' = n'q'$, then

$$gg' = nqn'q' = n(qn'q^{-1})qq' = n\theta(q)(n')qq'$$

Definition 3.4. A group G is a semidirect product of its subgroups N, Q if N is normal and $\pi\colon G \to G/N$ induces an isomorphism $\pi|_Q\colon Q \to G/N$. In this case we write $G = N \rtimes Q$.

Proposition 3.5. By definition, $G = N \rtimes Q$ if we have the following conditions
(1) $N \lhd G$.
(2) $NQ = G$.
(3) $N \cap Q = \{1\}$.

Proposition 3.6. If $G = N \rtimes Q$, we define an operation on $N \times Q$ by

$$(n, q)(n', q') = n\theta(q)(n')q'q$$

Then this operation makes $N \times Q$ a groups and its isomorphic to G.

Proof. We write ${}^q n$ for $\theta(q)(n)$. Then

$$((n, q)(n', q'))(n'', q'') = (n \cdot {}^q n' \cdot {}^{qq'} n'', qq'q'') = (n, q)((n', q')(n'', q''))$$

Hence the associative law holds. Since $\theta(1) = 1$ and $\theta(q)(1) = 1$,

$$(1, 1)(n, q) = (n, q) = (n, q)(1, 1)$$

So $(1, 1)$ is the identity element. Also,

$$(n, q)({}^{q^{-1}} n^{-1}, q^{-1}) = (1, 1) = ({}^{q^{-1}} n^{-1}, q^{-1})(n, q)$$

Therefore (n, q) has inverse. Thus $N \times Q$ is indeed a group in this way.

Consider $N \times Q \to G, (n, q) \mapsto nq$, then by previous discussion we know that this is a group isomorphism. In particular $N \times \{1\}$ corresponds to N and $\{1\} \times Q$ corresponds to Q. □

Example 3.7 (mapping torus)**.** Let X be a topological space, $f\colon X \to X$ is a homeomorphism and $I = [0, 1]$. We can construct the so called mapping torus

$$M_f = X \times I/((x, 0) \sim (f(x), 1))$$

$p\colon M_f \to S^1$ would be a fiber bundle with fiber X.

Now take $x_0 \in X$ and assume $f(x_0) = x_0$. If x_0 admits a contractible neighborhood $N \subset X$, we will show that

$$\pi_1(M_f, m_0) = \mathbb{Z} \rtimes \pi_1(X, x_0)$$

where $m_0 = \overline{(x_0, \frac{1}{2})} \in M_f$. The semidirect

4. Jordan–Hölder theorem