Algebra II

Naruki Masuda

April 21, 2025

Contents

Chapter 1

1

We first talk bout semidirect products. Let G be any group, and N, H be subgroups of G.

Definition 1.1. For $\varphi : H \to \mathrm{Aut}(N)$, define $N \rtimes H$ by

(1) $N \rtimes_\varphi H = N \times H$ as a set.

(b) Equipped with the group structure

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi(h_1)n_2, h_1h_2)$$

The structure $(N \rtimes_\varphi H, \cdot)$ forms a group.

Example 1.1. If N is a normal subgroup of G, and $N \cap H = \{e\}$, and $\varphi : H \to \mathrm{Aut}(N)$ where

$$\varphi : h \mapsto (n \mapsto hnh^{-1})$$

(acting by conjugation), and $G = NH$. Then

$$N \rtimes_\varphi H \to G$$

where

$$(n, h) \mapsto nh$$

is a bijective homomorphism homomorphism. Hence

$$G \cong N \rtimes_\varphi H$$

what is happening
Nxt we present some divisibility results.

Proposition 1.1 (Lagrange, Orbit-Stabilizer)**.** We have the following divisibility results:

- Let H be a subgroup of G, let $[G : H]$ denote the number of cosets of H in G, then

$$|G| = |H|[G : H]$$

- Let G be a finite group acting transitively on a finite set A, then for any $a \in A$, we have

$$|\mathrm{Stab}_G(a)| \cdot |O_G(a)| = |G|$$

The class formula is when G acts on itself by conjugation:

Proposition 1.2 (class formula). Let G act on a finite set S, and let $Z(G)$ denote the center of the group G, then

$$|S| = |Z(G)| + \sum_{a \in A} |O_G(a)|$$

where A includes exactly one element from each nontrivial orbit.

If G acts on itself by conjugation, then

$$|G| = |Z(G)| + \sum_{g} |[g]| = |Z(G)| + \sum_{g} \frac{|G|}{|C_G(g)|}$$

where $[g]$ denote the conjugacy class of g, and the sum includes exactly one from each nontrivial conjugacy class in G.

Problem 1.1 (F19-Q2). 2. Let p, q be two prime numbers such that $p \mid q-1$. Prove that

(a) there exists an integer $r \neq 1 \mod q$ such that $r^p \equiv 1 \mod q$;

(b) there exists (up to an isomorphism) only one noncommutative group of order pq.

Proof. (a) We want to show that there exists an element $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that

$$r^p \equiv 1 \mod q$$

We can do this because $(\mathbb{Z}/q\mathbb{Z})^\times$ has order $(q-1)$ and $p|(q-1)$. Therefore by Cauchy's theorem, there exists an element of order p in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Let n_p, n_q denote the number of p, q-Sylow subgroups. We see that $n_q|p$ and $n_q \equiv 1 \mod q$, since $p < q$, we must have $n_q = 1$. Now $n_p = 1$ or q by the same reasoning. Suppose $n_q = 1$, let P, Q denote the normal subgroups of order p, q, then

$$G \cong P \times Q$$

by a standard argument (included in the lemma below). Then G is commutative. Hence $n_p = q$. We therefore have what

□

Lemma 1.1. Let p, q be two primes such that $p < q$, and N, H has order p, q respectively, suppose that N is normal in G, and $N \cap H = \{e\}$, then

$$G \cong N \times H$$

Proof. We consider the map

$$\psi : N \times H \to G$$

such that

$$(n, h) \mapsto nh$$

We want to show that ψ is a homomorphism and ψ is injective (hence bijective by size argument). It is clearly injective:

$$nh = e \Rightarrow n, h \in N \cap H = \{e\}$$

It suffices to show that ψ is a homomorphism. We see that this implies

$$n_1 n_2 h_1 h_2 = n_1 h_1 n_2 h_2$$

Therefore it suffices to for any $n \in N, h \in H$, one has

$$nh = hn$$

Consider the conjugation action

$$\varphi : H \to \text{Aut}(N)$$

where

$$h \mapsto \left(n \mapsto hnh^{-1}\right)$$

Then we claim that φ is trivial. This is because $\ker(\varphi)$ has size either 1 or q. If it has size q, then the map is trivial; if it has size 1, then H embeds in $\text{Aut}(N)$, however, $|H| = q, \text{Aut}(N) = p-1$, and $q \nmid (p-1)$, hence impossible. This shows that the map is trivial, i.e., for $n \in N, h \in H$,

$$hn = nh$$

as desired. □

> **Problem 1.2** (F2015-Q1). Prove every group of order 15 is cyclic.

Proof. We will show that any group G of order 15 is isomorphic to

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

For this, using the above lemma, it suffices to show that there is one normal subgroup of order 3 and one normal subgroup of order 5. We repeat the argument above, $n_5 \mid 3$ and $n_5 \equiv 1 \mod 5$, hence $n_5 = 1$. Moreover, $n_3 \mid 5$ and $n_3 \equiv 1 \mod 3$, hence $n_3 = 1$ as well. By the lemma above, we know that

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

hence cyclic as desired. □

> **Problem 1.3** (S2015-Q2). Let p and q be primes with $p < q$. Let G be a group of order pq. Prove the following statements:
>
> (a) If p does not divide $q-1$ (i.e., $p \nmid q-1$), then G is cyclic.
>
> (b) If p divides $q-1$ (i.e., $p \mid q-1$), then G is either cyclic or isomorphic to a non-abelian group on two generators. Give the presentation of this non-abelian group.

Proof. This question is exactly the same as F19-Q2, we will only outline here.

(a) We have $n_q = 1$, and $n_p \mid q$, hence $n_p = 1$ or q, moreover $n_p \equiv 1 \mod p$. If $n_p = q$, this implies that $p \mid (q-1)$, hence $n_p = 1$. Therefore by the above argument

$$G \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$$

(b) If $p \mid (q-1)$, then $n_p = 1$ or q. Hence G is either of the form above or isomorphic to the non-abelian group

$$G = P \rtimes Q$$

not finished, what are the two generators

□

Problem 1.4 (F2007-Q1). Prove that no group of order 148 is simple.

Proof. We note the prime factorization of 148 is

$$148 = 2^2 \cdot 37$$

We see that $n_{37} \mid 4$ and $n_{37} \equiv 1 \mod 37$, therefore $n_{37} = 1$. This shows that there exists a normal subgroup of order 37, i.e., the group is not simple. □

Problem 1.5 (F2017-Q1). Show that there is no simple group of order 30.

Proof. This is slightly more complicated, and we will use a counting argument. Same reasoning as the above. The prime factorization of 30 is as below:

$$30 = 2 \cdot 3 \cdot 5$$

We see $n_5 \mid 6$, and $n_5 \equiv 1 \mod 5$. Unfortunately, n_5 could either be 1 or 6. Now $n_3 \mid 10$, and $n_3 \equiv 1 \mod 3$, unfortunately again n_3 could be 10. However, we argue that $n_3 = 10$ and $n_5 = 6$ cannot happen at the same time. Suppose this is the case, then there are 20 elements of order 2 and 24 elements of order 5, but this is too many! Hence either $n_3 = 1$ or $n_5 = 1$, as desired. □

Problem 1.6 (Richard Borcherds). All groups of order less than 60 are solvable, i.e., there exists a sequence of subgroups of G, $G_0, \ldots, G_k$ such that G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian, and

$$1 = G_0 \subset \cdots \subset G_k = G$$

...

Problem 1.7 (F2011-Q1).

(a) Let G be a group of order 5046. Show that G cannot be a simple group. You may not appeal to the classification of finite simple groups.

(b) Let p and q be prime numbers. Show that any group of order p^2q is solvable.

Proof. (a) The prime factorization of 5049 is as follows:

$$5049 = 2 \cdot 3 \cdot 29^2$$

Hence we see $n_{29} = 1$, i.e., there is a normal subgroup of order 29, therefore not simple.

(b) We will do discussion by cases.

(1) $p > q$. Then $n_p = 1$ or q and $n_p \equiv 1 \mod p$, therefore $n_p = 1$. Let P be the normal subgroup of G of order p^2, we thus have

$$\{e\} \subset P \subset G$$

It is clear that $|G/P| = q$, thus abelian, and $|P| = p^2$ also abelian as well (by the lemma below). This shows that G is solvable.

□

Lemma 1.2 (p^2 abelian). Fix prime p, any group of order p^2 is abelian.

Proof. □