Abstract Algebra – I Groups (群理论)

Melchior Grützmann / 古梅西

November 6, 2012

Outline

Exercise

a. Show that S_n is generated by (12), (23),..., $(n-1\ n)$.

b. Show that S_n is generated by (12) and $(12\ldots n)$.

Exercise

a. Show that $S_4 \cong \langle a, b : a^4 = \mathrm{id} = b^2 = (ba)^3 \rangle$.

b. Show that $A_4 \cong \langle a, b : a^3 = \mathrm{id} = b^2, aba = ba^2b \rangle$.

Exercise

How many k-cycles are there in S_n?

Exercise

Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 4 & 2 & 8 & 3 & 1 \end{pmatrix}$

a. Write σ as product of disjoint orbits. Determine its signum and its order.
b. What is the order of the centralizer of σ in S_8? What is the order of the conjugacy class of σ?

Exercise

a. List all conjugacy classes of S_5 together with their orders.
b. List all conjugacy classes of A_5 together with their orders.
Warning: There are even cycles of S_5 that are conjugate in S_5 but not in A_5.
c. Conclude that A_5 has no normal subgroup beside 1 and A_5.

Literature

- 里克正 (Li Kezheng): 抽象代数基础 *(Basic Algebra)*, Springer **(2007)**, Higher Education Press, ISBN 978-730-214-407-6
- P. A. Grillet: *Abstract algebra*, Graduate texts in mathematics (Springer, 2007), ISBN 978-038-771-567-4.
- 杨子胥 (Yang Zixu): 近世代数 *(International Algebra)*, 3rd edition, Higher Education Press **(2011)**, ISBN 978-704-030-072-7.
- written by the web: *Wikipedia the free encyclopedia*. en.wikipedia.org.

The Sylow theorems (西罗定理)

Long-term goal: classify all finite groups. Given the list of examples of finite groups we have obtained so far, it is clear that the difficult part are non-abelian indecomposable subgroups. A helpful tool is the theorem due to Peter Ludwig Mejdell Sylow[1]. Before we can state that theorem, we need to introduce some notions.

Definition

Given a prime $p \in \mathbb{P}$, then a finite group G is a p-group if $(G : 1) = p^k$ for some $k \in \mathbb{N}$.

By Lagrange's Theorem every element in a p-group has order p^k for some $k \in \mathbb{N}$ (Depending on the element).

[1] * 12/1832 in Norway, † 9/1918

Definition

Given a finite group G of order n and a prime $p \in \mathbb{P}$. Then a p-Sylow subgroup is a p-subgroup of maximal order p^k (for $k \in \mathbb{N}$) such that $p^k | n$, but not $p^{k+1} | n$.

Theorem

Given a finite group G of order n and a prime $p \in \mathbb{P}$. Then the following statements hold about p-Sylow subgroups.

1. *There exists at least one p-Sylow subgroup of G. If $p^k | n$, but not $p^{k+1} | n$, then every subgroup of order p^k is a p-Sylow subgroup.*
2. *All p-Sylow subgroups of G are conjugate.*
3. *The number n_p of p-Sylow subgroups of G is congruent 1 modulo p and $n_p | m$ where $n = mp^k$.*

Proof.

The proof covers the main part of this section. We follow a combinatorial proof sketched in [wiki, Sylow's theorems]. It consists of several lemmas.

Lemma

Let G be a finite p-group with an action on a finite set X. Let X_0 denote the set of fixed points. Then $|X| \equiv |X_0| \pmod{p}$.

Proof.

Write X as disjoint union of its orbits under G. Any element $x \in X \setminus X_0$ will lie in an orbit of order $|G|/|\operatorname{Stab}_G(x)|$ which is a multiple of G by the assumption of the lemma. The only orbits with sizes that are not multiples of p are the fixed points and thus the claim follows. □

Lemma

If $H \subset G$ is a finite p-subgroup and P is a p-Sylow subgroup, then there exists an element $g \in G$ such that $gHg^{-1} \subset P$.

Proof. II

Proof.

Let $X := G/P$ and let H act on X by left-multiplication. Applying the previous lemma to H acting on X, we see that $|X| \equiv |X_0| \pmod{p}$. Note that p does not divide $(G : P)$, because P is of maximal order, so p does not divide $|X_0|$. Therefore in particular $X_0 \neq \emptyset$ and we pick $gP \in X_0$. It follows that for every $h \in H$ we have $hgP = gP$ and so $g^{-1}hgP \subset P$. In total we obtain $g^{-1}Hg \subset P$ as claimed. □

Note that the last lemma implies that all p-Sylow subgroups are conjugate, because we can apply it twice to mutually embed conjugates of the p-Sylow subgroups into each other.

In order to prove the last statement in the theorem, note that the first lemma implies $n_p = [G : N_G(P)]$ where P is any p-Sylow subgroup and $N_G(P)$ is the normalizer of P in G.

Proof. III

Since $P \subset N_G(P) \subset G$ we have $n_p | m$ as stated in the theorem. Let $X = \mathrm{Syl}_p(G)$ the set of all p-Sylow subgroups of G and let P act on X by conjugation. Let $Q \in X_0$ with X_0 the fixed-point set. Note that this implies $gQg^{-1} = Q$ for all $g \in P$. Therefore $P \subset N_G(Q)$. By the last lemma P and Q are conjugate in G. Since Q is normal in $N_G(Q)$, we have $P = Q$. Therefore $X_0 = \{P\}$ and so by Lemma 1 the Theorem follows. □

Proof. III

Since $P \subset N_G(P) \subset G$ we have $n_p | m$ as stated in the theorem. Let $X = \mathrm{Syl}_p(G)$ the set of all p-Sylow subgroups of G and let P act on X by conjugation. Let $Q \in X_0$ with X_0 the fixed-point set. Note that this implies $gQg^{-1} = Q$ for all $g \in P$. Therefore $P \subset N_G(Q)$. By the last lemma P and Q are conjugate in G. Since Q is normal in $N_G(Q)$, we have $P = Q$. Therefore $X_0 = \{P\}$ and so by Lemma 1 the Theorem follows. □

It is not necessary to remember the whole proof for the exams. However the Theorem as well as some results of the lemmas in the proof can be helpful for proving things in the exam, the homework or in research about finite groups.

Example I

Given a group of order 15 show that it is isomorphic to $\mathbb{Z}/(15)$. The problem is of course to show that the group is abelian. We start with $15 = 3 \cdot 5$ and observe that $n_5|3$ and $n_5 \equiv 1 \pmod 5$ implies $n_5 = 1$. Therefore the only subgroup of order 5 is normal as it has no distinct conjugates. Similarly $n_3|5$ and $n_3 \equiv 1 \pmod 3$ imply $n_3 = 1$. Therefore also the only subgroup of order 3 is normal. Since the intersection of these two normal subgroups is $\{\mathrm{id}\}$, G must be a direct product of the groups of order 3 and 5. Therefore $G \cong \mathbb{Z}/(3) \times \mathbb{Z}/(5) \cong \mathbb{Z}/(15)$.

Corollary

A finite group is a p-group iff every element has order a power of p.

Proof.

The Sylow theorem implies in particular that for $n = p_1^{n_1} \dots p_k^{n_k}$ with $p_i \in \mathbb{P}$ distinct primes and $n_i \in \mathbb{N}_+$, there are subgroups of order $p_i^{n_i}$. It is easy to see that such a subgroup must contain an element of order p_i^N for some $N \in \mathbb{N}_+$, $N \leq n_i$. □

Exercises I

Exercise

Given a finite group whose order is divisible by a prime p. Show that there is a subgroup of order p.

Exercise

Find the Sylow subgroups of

a. S_4 and
b. S_5.

Exercise

Find all groups of order

a. 33,
b. 35,
c. 45.

Exercises II

Exercise

Show that the following are not simple groups, i.e. that they have a non-trivial normal subgroup:

a. A group of order 18;

b. A group of order 30;

c. A group of order 56.