KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-02-16

MATS BOIJ

4. The fourth lecture - Lagrange's Theorem and finitely generated abelian groups

In the fourth lecture, we start by studying cosets of a subgroup in order to get to Lagrange's theorem and to prepare for making factor groups. Then we look at direct products and the structure theorem for finitely generated abelian groups.[1]

Definition 4.1 (Cosets)**.** Let H be a subgroup of a group G. The *left-cosets of H in G* are the subsets of G that can be written as

$$gH = \{gh | h \in H\}$$

for some element g in G. Similarly, *right-cosets of H in G* are the subsets of G that can be written as

$$Hg = \{hg | h \in H\}$$

for some element g in G. $G/_L H$.

It turns out the the cosets are the equivalence classes of natural equivalence relations on G defined by the subgroup H.

Theorem 4.2. *The relation given by $a \sim_L b \Leftrightarrow a^{-1}b \in H$ is an equivalence relation with the left cosets of H as its equivalence classes.*

Similarly, the right cosets of H are the equivalence classes of $a \sim_R b \Leftrightarrow ab^{-1} \in H$.

In particular, the cosets give two partitions of the set G into disjoint subsets.

Proof. We first check that the relations are equivalence relations:

$i)$ (*reflexivity*) $a^{-1}a = aa^{-1} = e \in H$, for all $a \in G$.

$ii)$ (*symmetry*) $(a^{-1}b)^{-1} = b^{-1}a$ and hence $a^{-1}b \in H \Leftrightarrow b^{-1}a \in H$ since H is a subgroup. We also get $(ab^{-1})^{-1} = ba^{-1}$ and $ab^{-1} \in H \Leftrightarrow ba^{-1} \in H$.

$iii)$ (*transitivity*) If $a^{-1}b \in H$ and $b^{-1}c \in H$, we get $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. Moreover, if $ab^{-1} \in H$ and $bc^{-1} \in H$, we get $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$.

[1]The fourth lecture is based on the sections 10-11 of Chapter II in A First Course in Abstract Algebra [1].

Now, we check that $a \sim_L b$ if and only if they are in the same coset. In fact, $a^{-1}b \in H \Leftrightarrow b \in aH$. In the same way

$$ab^{-1} \in H \Leftrightarrow a \in Hb.$$

Since the equivalence classes give a partition of the set, we get that the cosets give two partitions of the set G into disjoint subsets. □

Theorem 4.3 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$ a subgroup, then $|H|$ is a divisor in $|G|$.*

Proof. We know from above that the left cosets of H form a partition of disjoint subsets. It is now sufficient to see that all the cosets have the same cardinality. In fact, we have that left multiplication by g gives a bijection

$$H \longrightarrow gH.$$

□

Definition 4.4 (index)**.** The *index* of a subgroup H in the group G is the number of left (or right) cosets of H in G and is denoted by $(G : H)$.

Exercise 4.5. *Show that even if the group G is infinite, the index of a subgroup may be finite and in that case, the number of left and right cosets are the same.*

Corollary 4.6. *$a^{|G[} = e$ for any element a of a finite group G, i.e., the order of a divides the order of G.*

Proof. The cyclic subgroup generated by a has an order which is the order of a. Because of Lagrange's theorem, we have that the order of $\langle a \rangle$ divides the order of G. □

As an easy consequence of Lagranges theorem, we get the following useful result from number theory:

Theorem 4.7. *Let n be any positive integer then we have that*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for all integers a relatively prime to n, where $\phi(n)$ denotes the number of positive integers less than n which are relatively prime to n.

Proof. Let $\mathbb{Z}_n^*$ denote the set of residue classes module n which are relatively prime to n. These are the invertible elements in $\mathbb{Z}_n$ under multiplication and they hence form a group. The order of this multiplicative group is $\phi(n)$, since this is the number of invertible residue classes modulo n. □

Corollary 4.8 (Fermat's Theorem)**.** *$a^p \equiv a \pmod{p}$ if a is an integer and p is a prime.*

4.1. **Direct products.**

Definition 4.9 (Direct product)**.** If G and H are groups, we can define a group structure on the Cartesian product, $G \times H$, by componentwise operations:

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2),$$

for $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

More generally, we can define this for any collection of groups $\{H_i\}_{i \in I}$ and we get the *direct product* $\prod_{i \in I} H_i$.

Remark 4.10. The direct product is associative in the sense that

$$H_1 \times (H_2 \times H_3) \cong (H_1 \times H_2) \times H_3 \cong \prod_{i=1}^{3} H_i.$$

Theorem 4.11. *The group $\prod_{i=1}^{k} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ if and only if the numbers $m_1, m_2, \ldots, m_k$ are pairwise relatively prime.*

Proof. The element $(1, 1, \ldots, 1)$ has an order which is the least common multiple of the orders of the factors. Hence if the numbers are pairwise relatively prime, the product is cyclic.

If there is a common factor between any two of the numbers $m_1, m_2, \ldots, m_k$, we can find non-trivial elements of the same order in two of the factors. These elements generates different subgroups of the same order in the product, which cannot be cyclic by the characterization of cyclic groups. $\square$

Definition 4.12 (Free abelian group)**.** For any set S let $F_S = \prod_{i \in S} \mathbb{Z}$ be the *free abelian group* on S. (This is the same as the group of integer functions on S under pointwise addition.)

Exercise 4.13. *Show that for any abelian group A with a generating set S, there is a a surjective group homomorphism*

$$F_S \longrightarrow A.$$

Theorem 4.14 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Any finitely generated abelian group is a direct product of cyclic groups.*

We will not prove this theorem completely now, but will look at some ingredients that goes into it.

Lemma 4.15. *Let A be an abelian group of order n and for any prime divisor p of n, denote by A_p the set of elements in A of p power order. Then $A \cong \prod_{p|n} A_p$.*

Proof. Write $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where $p_1, p_2, \ldots, p_k$ are the distinct prime divisors of n. Let $q_i = n/p_i^{n_i} = \prod_{j \neq i} p_j^{n_j}$.

Define a homorphism

$$\Phi : A_{p_1} \times A_{p_2} \times \cdots A_{p_k} \longrightarrow A$$

by $\Phi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$.

Assume that $a = a_1 + a_2 + \cdots + a_k = 0$. Then we have that $q_i a = q_i a_i = 0$, for all $i = 1, 2, \ldots, k$. But, $q_i a_i = 0 \Leftrightarrow a_i = 0$, since a_i has p_i power order. Hence Φ is injective.

To see that Φ is surjective, we can find an integer $m = \sum_{i=1}^k b_i q_i$ such that $m \equiv 1 \pmod{n}$. For such an element we have that

$$a = ma = \sum_{i=1}^k b_i q_i a = \sum_{i=1}^k a_i$$

where $a_i = b_i q_i a \in A_{p_i}$, for $i = 1, 2, \ldots, k$.

To find such an integer m, we note that $\prod_{i=1}^k \mathbb{Z}_{p_i^{n_i}} \cong \mathbb{Z}_n$ via the homomorphism

$$\Psi(b_1, b_2, \ldots, b_k) = \sum_{i=1}^k b_i q_i,$$

where it is sufficient to check injectivity because the two groups have the same order. $\Psi(b_1, b_2, \ldots, b_k) = 0$ implies that b_i is divisible by $p_i^{n_i}$ for each i since all the terms $b_j q_j$ are divisible by p_i for $j \neq i$. Hence Ψ is injective. □

This lemma reduces the study of finite abelian groups to the study of abelian groups of prime power order, i.e., abelian p-groups.

Recommended excercises

II-10 Cosets and the Theorem of Lagrange. 17-19, 28-33, 36, 37, 39, 40, 44, 46, 47

II-11 Direct Products and Finitely Generated Abelian Groups. 32, 34, 36, 47, 49

II-12 Plane Isometries. [2] 16-20, 24-37

References

[1] J. B. Fraleigh. *A First Course In Abstract Algebra*. Addison Wesley, seventh edition, 2003.

[2] This section can be seen as an application of what has been done so far and there is no lecture covering this section.