KTH Teknikvetenskap

SF2729 GROUPS AND RINGS LECTURE NOTES 2010-02-23

MATS BOIJ

5. The fifth lecture - Homomorphisms and Factor Grouops

In the fifth lecture, we start by a quick look at homomorphisms and go furher to define factor groups which are quotients of a group by a normal subgroup. The elements of the factor groups are cosets. We will end by using this to prove the structure theorem for finitely generated abelian groups.[1]

Definition 5.1 (Homomorphism, kernel and image)**.** A *group homomorphism* is a function $\phi : G \longrightarrow H$ between groups preserving the gruop structure, i.e., satisfying

$$\phi(a *_G b) = \phi(a) *_H \phi(b), \qquad \forall a, b \in G.$$

The kernel of ϕ is given by

$$\ker \phi = \{a \in G | \phi(a) = e_H\}$$

and the *image* of ϕ is given by

$$\mathrm{im}\phi = \{\phi(a) | a \in G\}.$$

Remark 5.2. More generally, we can define $\phi(K) \leq H$ as

$$\phi(K) = \{\phi(a) | a \in K\}$$

for any subgroup $K \leq G$ and

$$\phi^{-1}(K) = \{a \in G | \phi(a) \in K\}$$

for any subgroup $K \leq H$.

Example 5.3. The exponential function is a homomorphism $\exp : \mathbb{C} \longrightarrow \mathbb{C}^*$. We have that the unit circle S^1 is a subgroup in $\mathbb{C}^*$ and the inverse image of S^1 under the exponential map is the imaginary axis $i\mathbb{R}$ in $\mathbb{C}$.

Example 5.4. The exponential map $\exp : M_2(\mathbb{R}) \longrightarrow \mathrm{Gl}_2(\mathbb{R})$ is not a homomorphism, but induces a homomorphism on the subset of skew-symmetic matrices. The image is the special orthogonal group $\mathrm{SO}_2(\mathbb{R})$.

[1]The fifth lecture is based on the sections 13-15 of Chapter II in A First Course in Abstract Algebra [1].

Definition 5.5 (Normal subgroup)**.** A subgroup $H \leq G$ is *normal* if the left and right cosets are the same, i.e. if any of the following three equivalent conditions holds:

$i)$ $aH = Ha$, for all $a \in G$.
$ii)$ $aHa^{-1} = H$, for all $a \in G$.
$iii)$ $a^{-1}Ha = H$, for all $a \in G$.

Remark 5.6. All subgroups of an abelian group are normal.

Theorem 5.7. *The kernel of a homomorphism $\phi : G \longrightarrow H$ is a normal subgroup in G.*

Proof. If a is any element in G and $b \in \ker \phi$, we have that

$$\phi(a^{-1}ba) = \phi(a^{-1})e_H\phi(a) = \phi(a^{-1}a)) = \phi(e_G) = e_H$$

Hence $a^{-1}ba \in \ker \phi$ and $\ker \phi$ is normal in G. □

We will soon see that any normal subgroup is the kernel of some homomorphism.

Definition 5.8 (Factor group)**.** Let $H \leq G$ be a normal subgroup. The *factor group*, or *quotient group*, G/H is the set of cosets of H with the binary operation given by

$$aH * bH = abH,$$

for a, b in G.

Remark 5.9. We have to check that the binary operation is well defined. We can see this since $(aH)(bH) = a(Hb)H = abHH = abH$ since H is normal. The operation is associative since the operation on G is associative, and the coset $H = eH$ is a unit. The inverse of aH is given by $a^{-1}H$. Hence the factor group is in fact a group.

Theorem 5.10. *If $H \leq G$ is a normal subgroup, there is a natural quotient homomorphism $G \longrightarrow G/H$ whose kernel is H.*

Proof. The homomorphism $\phi : G \longrightarrow G/H$ is given by $\phi(a) = aH$. Because of the definition of the operation on G/H we have that

$$\phi(ab) = abH = aHbH = \phi(a)\phi(b), \qquad \forall a, b \in G.$$

The kernel of ϕ is given by

$$\ker \phi = \{a \in G | aH = H\} = \{a \in G | a \in H\} = H.$$

□

Theorem 5.11 (Isomorphism theorem)**.** *If $\phi : G \longrightarrow H$ is a group homomorphism we have an isomorphism*

$$G/\ker \phi \xrightarrow{\sim} \mathrm{im}\phi.$$

Proof. Let $K = \ker \phi$ and define a homorphism

$$\Phi : G/K \longrightarrow H$$

by $\Phi(aK) = \phi(a)$, for $a \in G$. This is well-defined since if $aK = bK$, we have $ab^{-1} \in K$ and $\phi(ab^{-1}) = e_H$. Hence $\phi(a) = \phi(b)$.

The homomorphism Φ is injective since the kernel of Φ is given by

$$\ker \Phi = \{aK \in G/K | aK = K\} = \{K\}.$$

Thus Φ gives an isomorphism of G/K onto the image $\mathrm{im}\Phi = \in \phi$. $\square$

Example 5.12. We have seen that the alternating grop A_n is a subgroup of the symmetric group S_n. In fact, it is normal since it is the kernel of the homomorphism $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$. By Theorem 5.11 we get that the factor group S_n/A_n is isomorphich to the image, $\{\pm 1\}$ when $n \geq 2$.

Example 5.13. Since the special linear group $\mathrm{Sl}_n(\mathbb{R})$ is the kernel of $\det : \mathrm{Gl}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$, we get that $\mathrm{Sl}_n(\mathbb{R})$ is a normal subgroup and by Theorem 5.11 the factor group $\mathrm{Gl}_n(\mathbb{R})/\mathrm{Sl}_n(\mathbb{R})$ is isomorphic to the image, $\mathbb{R}^*$.

Example 5.14. The three permutations of type $[2^2]$ form a subgroup H of $G = S_4$ together with the identity permutation. Thus subgroup is normal since the type is preserved under conjugation. The quotient G/H has order $24/4 = 6$ and since there is no element of order 6 in S_4, there can be no element of order 6 in the factor group G/H. Hence G/H has to be isomorphic to S_3 and there is a homomorphism from S_4 to S_3 whose kernel is H.

Definition 5.15. (Center) The *center* of a gruop G is the subgroup given by

$$Z(G) = \{a \in G | ab = ba, \quad \forall b \in G\}$$

Theorem 5.16. *The center, $Z(G)$, is a normal subgroup og G.*

Proof. First check that $Z(G)$ is a subgroup. If $a, b \in Z(G)$, and c is any element of G, we get that

$$(ab^{-1})c = a(c^{-1}b)^{-1} = a(bc^{-1})^{-1} = acb^{-1} = cab^{-1} = c(ab^{-1})$$

which shows that $ab^{-1} \in Z(G)$.

Now if $a \in Z(G)$ and b is any element of G, we have

$$bab^{-1} = abb^{-1} = a \in Z(G)$$

which shows that $bZ(G)b^{-1} = Z(G)$ and $Z(G)$ is normal. $\square$

Definition 5.17 (Simple group). A group is *simple* if it has no proper non-trivial normal subgroups.

Remark 5.18. Note that this means that all homomorphisms from a simple group are injective or trivial.

Finitely generated abelian groups. In the previous lecture we looked at the structure theorem for finitely generated abelian groups. Now we are in a situation where we can understand why this theorem holds using factor groups.

Theorem 5.19. *A finitely generated abelian group is isomorphic to $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \times \mathbb{Z}^r$, where $m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$ and $r \in \mathbb{N}$ are such that m_i divides m_{i+1} for $i = 1, 2, \ldots, k-1$.*

Sketch of proof. Let A be a finitely generated abelian gruop written additively. Since A is finitely generated, we have a surjective homomorphism from a free abelian gruop $\mathbb{Z}^n$ to A. Let K be the kernel of this homomorphism. We can find a homomorphism from a free abelian group F to $\mathbb{Z}^n$ mapping onto K and we can think of K being generated by the rows of a matrix with n columns and possiby infinitely many rows.

Let m_1 be the smallest positive integer in the subgroup of $\mathbb{Z}$ genereted by all the entries of the matrix. Then any other element in the matrix is divisible by m_1 and by elementary row and column operations we can arrange so that m_1 appears in the top left corner. Now we can use such operatations again to eliminate everything else from the first row and first column. By induction on n we can proceed to get a diagonal matrix with entries $m_1, m_2, \ldots, m_k$ in the top left corner and the rest of the matrix zero. Moreover, m_i divides m_j for all $1 \leq i \leq j \leq k$.

The row and column operations only changes bases in the free abelian groups, but we have not obtained a homomorphism $\Phi : \mathbb{Z}^k \longrightarrow \mathbb{Z}^n$ such that the image is isomorphic to K after a change of bases in $\mathbb{Z}^n$, which in turn corresponds to another choice of generators in A.

The theorem now follows from the isomorphism theorem since A is isomorphic to $\mathbb{Z}^n/K \cong \mathbb{Z}^n/\mathrm{im}\Phi$. □

Remark 5.20. The *rank* of A is the number r in the previous theorem and we see from the proof that $r = n - k$. Some of the numbers $m_1, m_2, \ldots, m_k$ may be equal to 1 and these copies of the trivial group $0 = \mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z}$ may be omitted and we can get the same statement with the additional condition that $m_1 > 1$.

RECOMMENDED EXCERCISES

III-13 Homomorphisms. 32, 39-45, 47,48, 50, 52

III-14 Factor groups. 23, 24, 30, 31, 33-36, 40

III-15 Factor-Groups Computations and Simple Groups. 19-23, 34-36, 39

REFERENCES

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