KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-03-09

MATS BOIJ

7. The seventh lecture - Isomorphism Theorems, Free Groups and Group Presentations

In the seventh lecture, which is the last of the lectures in the first part of the course, we start by looking at the isomorphism theorems and then proceeed to free groups and group presentations. [1]

We recall the first isomorphism theorem from the fourth lecture:

Theorem 7.1 (First 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 $\mathrm{im}\Phi = \in \phi$. □

We will state the second isomorphism theorem as in [1] which is slightly more general than in [2]. In order to do this, we need the following definition.

Definition 7.2 (Normalizer)**.** The normalizer of a subgroup $H \leq G$ is given by

$$N_G(H) = \{a \in G | aHa^{-1} = H\} = \{a \in G | aH = Ha\}.$$

Exercise 7.3. *Show that $N_G(H)$ is a subgroup containing H and that it is the largest subgroup containing H in which H is normal. In particular, H is normal if and only if $N_G(H) = G$.*

[1]The sixth lecture is based on the sections 34, 38-40 of Chapter VII in A First Course in Abstract Algebra [2].

Theorem 7.4 (Second Isomorphism theorem). *If K and H are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G, K is normal in HK and $H \cap K$ is normal in H. Furthermore we have that*

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. We start by checking that HK is a subgroup. If $h_1, h_2 \in H$ and $k_1, k_2 \in K$ we get

$$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}k_1'k_2'$$

for some $k_1', k_2' \in K$, since $H \leq N_G(K)$. Hence HK is a subgroup.

Next, we check that K is normal in HK which follows from

$$hkk'(hk)^{-1} = hkk'k^{-1}h^{-1} = hh^{-1}k'' = k''$$

for some k'' in K since $H \leq N_G(K)$.

Now, we check that $H \cap K$ is normal in H. If $k \in H \cap K$ and $h \in H$ we get that $hkh^{-1} \in H$ since $h, k \in H$, but also $hkh^{-1} \in K$ since $H \leq N_G(K)$. Therefore $hkh^{-1} \in H \cap K$ and $H \cap K$ normal i H.

Finally, we will prove the isomorphism. In order to do this, we construct a homomorphism

$$\Phi : HK \longrightarrow H/H \cap K$$

by

$$\Phi(hk) = hH \cap K, \qquad \forall h \in H, \forall k \in K.$$

This is well-defined since $h_1k_1 = h_2k_2$ implies that $h_1^{-1}h_2 = k_1k_2^{-1}$ which is in $H \cap K$. It is a homomorphism since

$$\Phi(h_1k_1h_2k_2) = \Phi(h_1h_2k_1'k_2) = h_1h_2H \cap K = (h_1H \cap K) * (h_2H \cap K),$$

for all h_1, h_2 in H and all k_1, k_2 in K.

Since Φ is surjective it is by the First Isomorphism Theorem sufficient to show that $\ker \Phi = K$. We have that

$$\ker \Phi = \{hk \in HK | h \in H \cap K\} = K,$$

which finishe the proof. ∎

Theorem 7.5 (Third Isomorphism Theorem). *If $H \leq K$ are normal subgroups of G we have that*

$$\frac{G/H}{K/H} \cong G/K.$$

Proof. We can construct a homomorphism

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

by

$$\Phi(gH) = aK$$

for all a in G. It is well-defined since $a_1H = a_2H$ implies that $a_1^{-1}a_2 \in H$, but since $H \leq K$ we get $a_1K = a_2K$. For $a_1, a_2 \in G$ we have that

$$\Phi(a_1H * a_2H) = \Phi(a_1a_2H) = (a_1a_2)K = a_1K * a_2K$$

which shows that Φ is a homomorphism. Since Φ is surjective it is by the First Isomorphism Theorem sufficient to show that $\ker \Phi = K/H$. Since the unit in G/K is the coset eK, the kernel is given by

$$\ker \Phi = \{aH | aK = eK\} = \{aH | a \in K\} = K/H,$$

which finishes the proof. □

In the fourth lecture, we also looked at the proof of the structure theorem for finitely generated abelian groups. It was needed to present these groups as quotients of free abelian groups.

If we like to study groups in general, we have to use something more general than free abelian groups and therefore we introduce *free groups*.

Definition 7.6 (Free group)**.** Let A be any set (which we will call an *alphabet*) and define $F[A]$ to be the set of all finite words $a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m}$, where $a_1, a_2, \ldots, a_m \in A$ and $n_1, n_2, \ldots, n_m \in \mathbb{Z}$ modulo the equivalence relation generated by

$$a^m a^n = a^{m+n}, \qquad \forall m, n \in \mathbb{Z}$$

for subwords. The empty word is equivalent to a^0 for any $a \in A$ and is denoted by e.

Composition of words gives a group structure on $F[A]$ with e as a unit. This group is called the *free group on the alphabet A*.

The idea is that in a free group the symbols in the alphabet A satisfiy no relations apart from $a^m a^n = a^{m+n}$. This is similar to the situation with free abelian groups, where we have no other relations than $a + b = b + a$, between the generators.

Theorem 7.7. *For any group G there is a set A and a surjective homomorphism $F[A] \longrightarrow G$. In particular, any group is the factor group of a free group by a normal subgroup.*

Proof. Let A be a subset of G such that $G = \langle A \rangle$, i.e., A is a set of generators of G. We now define $\Phi : F[A] \longrightarrow G$ by

$$\Phi(a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m}) = a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m}$$

where the argument of Φ is a word in the alphabet A in $F[A]$ while the right hand side is a product which is in G. If two words are equivalent, they will map to the same element in G since such an equivalence corresponds to a relation which is valid in any group.

Since the group operation on $F[A]$ is given by composition of words, Φ is a homomorphism.

Since $\langle A \rangle = G$, we get that Φ is surjective and the First Isomorphism Theorem tells us that $G \cong F[A]/\ker \Phi$. □

Example 7.8. The free abelian group F_A is generated by A and therefore we have a surjective homomorphism

$$\Phi : F[A] \longrightarrow F_A.$$

The kernel $\ker \Phi$ is the smallest normal subgroup containing all the commutators $aba^{-1}b^{-1}$, for $a, b \in A$.

Definition 7.9 (relation, presentation)**.** A *relation* in a group generated by a subset A is an equality

$$a_1^{n_1}a_2^{n_2}\cdots a_k^{n_k} = b_1^{m_1}b_2^{m_2}\cdots b_\ell^{m_\ell}, \qquad a_i, b_j \in A, n_i, m_j \in \mathbb{Z}.$$

All such relations can be rewritten as

$$a_1^{n_1}a_2^{n_2}\cdots a_m^{n_m} = e$$

and we denote the relation by the word on the left hand side as an element of $F[A]$.

If we have a set of relations $S = \{r_i\}_{i\in I} \subseteq F[A]$, we can let R be the smallest normal subgroup containing S. If R is the kernel of the homomorphism $\Phi : F[A] \longrightarrow G$ given by Theorem 7.7 we say that the generators A together with the relations $S = \{r_i\}_{i\in I}$ give *group presentation* of G.

Example 7.10. We can use the idea of group presentations to study groups of order $2p$, where p is an odd prime. There is only one abelian group in this case, $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$.

Now assume that G is non-abelian of order $2p$. We have elements of order 1, 2 and p. Let a be any element of order p and b be any element of order 2. G is generated by $\{a, b\}$ since there can be no proper subgroup containing an element of order 2 and an element of order p.

The subgroup $H = \langle a\rangle$ has to be normal. (If $K = gHg^{-1} \neq H$ we get that $H \cap K = \{e\}$ and $|HK| = p^2$ since $|HK| = |H|| \cdot |K|/|H \cap K|$. However HK is a subset of G, so $p^2 < 2p$ gives a contradiction.)

Since b has order two, we have that $b = b^{-1}$ and since $H = \langle a\rangle$ is normal we get that $bab = a^k$, for some $k = 0, 1, 2, \ldots, p-1$. Thus we can say that G has a presentation

$$(a, b|a^p = e, b^2 = e, bab = a^k) = (a, b|a^p = e, b^2 = e, ba = a^k b)$$

for some $k = 0, 1, \ldots, p-1$.

Using the relation $b^2 = e$ we get that

$$a = b^2a = b(ba) = ba^kb = a^{k^2}b^2 = a^{k^2}.$$

using the relation $ba = a^kb$ several times. Since a has prime order p, we know that $k^2 \equiv 1 \pmod p$. This equation has only two solutions in the field $\mathbb{Z}_p$ and we get $k = 1$ or $k = p-1$. In the first case we have $ba = ab$, which implies that G is abelian contradicting our assumption. Thus we are left with only one non-abelian group of order $2p$, which is the Dihedral group D_{2p} with the presentation

$$(a, b|a^p = e, b^2 = e, bab = a^{-1})$$

Recommended excercises

VII-34 Isomorphism Theorems. 7-9

VII-38 Free Abelian Groups. 11, 16-18

VII-39 Free Groups. 11

VII-40 Group Presentations. 10,11

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.
[2] J. B. Fraleigh. *A First Course In Abstract Algebra*. Addison Wesley, seventh edition, 2003.