MA441: Algebraic Structures I

Lecture 26

10 December 2003

(page 179)

Example 13: A_4 has no subgroup of order 6. BWOC, suppose $H < A_4$ has order 6. Then $H \lhd A_4$, since it has index 2.

Thus A_4/H has order 2. For all $\alpha \in A_4$, $(\alpha H)^2 = (\alpha^2)H = H$, so $\alpha^2 \in H$.

However, there are nine distinct elements in A_4 of the form g^2. They can't all be in a subgroup of order 6, so we have a contradiction. (See the group table, p. 104.)

Alternatively, (page 139, Example 4):
let α be a 3-cycle, of which there are eight in A_4. Then $H, \alpha H, \alpha^2 H$ can't all be distinct. Any two of the three being equal implies $\alpha \in H$.

Therefore there would have to be eight 3-cycles in H of order 6.

This is a nice counterexample to the converse of Lagrange's theorem.

Review from Lecture 25:

Theorem 10.3:
The First Isomorphism Theorem
(Jordan, 1870)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then the mapping

$$G_1/(\mathsf{Ker}\,\phi) \to \phi(G_1)$$

given by

$$g_1\,\mathsf{Ker}\,\phi \mapsto \phi(g_1)$$

is an isomorphism, that is,

$$G_1/(\mathsf{Ker}\,\phi) \approx \phi(G_1).$$

Theorem 10.4:
Normal Subgroups are Kernels
Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup $N \lhd G$ is the kernel of the mapping $g \mapsto gN$ from G to the quotient group G/N.

Definition:
Two elements a, b in a group G are **conjugate** in G if for some $x \in G$, $b = xax^{-1}$. We say b is a conjugate of a (and vice-versa).

The **conjugacy class** of a, denoted $\mathrm{cl}(a)$ is the set of all conjugates of a, that is,

$$\mathrm{cl}(a) = \{xax^{-1} | x \in G\}.$$

Conjugacy is an equivalence relation, and the conjugacy classes partition a group.

Definition:
The **normalizer** of $H < G$ is denoted $N(H)$ and defined as

$$N(H) = \{x \in G | xHx^{-1} = H\}.$$

Even if H is not normal in G, $H \lhd N(H)$, and the normalizer is the largest subgroup of G that contains H as a normal subgroup.

Definition:
The **centralizer** of $H < G$ is denoted $C(H)$ and defined as

$$C(H) = \{x \in G | xhx^{-1} = h, \forall h \in H\}.$$

The centralizer of H is the subgroup consisting of all elements that commute with elements of H.

Theorem 9.5: Cauchy's Theorem (Abelian) Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

We'll prove Cauchy's Theorem for any finite group.

(page 396)

Theorem 24.1: The Number of Conjugates of a

Let G be a finite group and let a be an element of G. Then

$$|\,\mathrm{cl}(a)| = |G : C(a)|.$$

Proof:
Let T be the map that sends the coset $xC(a)$ to the conjugate xax^{-1} of a.

We will show that T is a bijection, which will show the number of conjugates of a is the same as the number of cosets of $C(a)$.

Well-defined: Suppose $xC(a) = yC(a)$. We want to show that the image under T does not depend on what representative we choose. That is, we want $xax^{-1} = yay^{-1}$.

Since $xC(a) = yC(a)$, that means $x^{-1}y \in C(a)$, or $(x^{-1}y)a = a(x^{-1}y)$.

Right multiply by y^{-1} to get $x^{-1}yay^{-1} = ax^{-1}$. Left multiply by x to get $yay^{-1} = xax^{-1}$.

One-to-one: reverse the argument

Onto: any conjugate of a has the form xax^{-1}, and thus has the preimage $xC(a)$ under T.

Note that conjugacy is an equivalence relation. This means that we can partition a group into conjugacy classes.

Reflexive: a is conjugate to itself.

Symmetric: If $a = xbx^{-1}$, then $b = x^{-1}a(x^{-1})^{-1}$. So if a is conjugate to b, then b is conjugate to a.

Transitive: If $a = xbx^{-1}$ and $b = ycy^{-1}$, then $a = (xy)c(xy)^{-1}$. So if a is conjugate to b and b is conjugate to c, then a is conjugate to c.

Corollary: The Class Equation

For any finite group G,

$$|G| = \sum |G : C(a)|,$$

where the sum runs over one representative element a from each conjugacy class of G.

If $a \in Z(G)$, then $C(a) = G$, and $|G : C(a)| = 1$. That is, the conjugacy class of an element in the center of G is just that element.

We can rewrite the class equation as

$$|G| = |Z(G)| + \sum |G : C(a)|,$$

where the sum runs over one representative element a from each conjugacy class of G that has more than one element, i.e., $a \notin Z(G)$.

Cauchy's Theorem

Let G be a finite group and p a prime that divides the order of G. Then G has an element of order p.

Proof:
We prove this by induction on the order of G. The statement is trivially true for $|G| = 1, 2$.

Assume the statement is true for groups of order less than $|G|$.

Suppose G has a proper subgroup $H < G$ whose order is divisible by p. Then by the induction hypothesis, H would have an element of order p, and we would be done. Therefore, we can assume that no proper subgroup of G has order divisible by p.

Consider the class equation for G:

$$|G| = |Z(G)| + \sum |G : C(a)|.$$

where the sum runs over a representative a of each conjugacy class of G for $a \notin Z(G)$.

Since $C(a) < G$, we can assume p does not divide $|C(a)|$.

We know

$$|G| = |C(a)| \cdot |G : C(a)|.$$

Since p divides $|G|$ and p does not divide $|C(a)|$, then p divides $|G : C(a)|$ for all $a \notin Z(G)$.

Now in the class equation

$$|G| = |Z(G)| + \sum |G : C(a)|,$$

we have that p divides $|G|$ and all terms of the sum. Therefore p divides $|Z(G)|$.

Since $Z(G)$ is an abelian group, we can apply Cauchy's Theorem in the abelian case to get an element of order p.

Cauchy's Theorem is a special case of a larger result.

Theorem 24.3:
Sylow's First Theorem (1872) on the Existence of Subgroups of Prime-Power Order

Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

(We skip the proof. You can read it on page 399.)

(page 211)

Theorem 11.1: The Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

(We skip the proof.)

With this theorem, we can classify all finite abelian groups of order n up to isomorphism. Let G be abelian of order n.

Then G determines primes $\{p_i\}$ (not necessarily distinct) and powers $\{n_i\}$ such that n factors as $p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ and such that

$$G \approx \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}.$$

(Order of terms does not matter up to isomorphism.)

We can list all possible isomorphism classes for abelian groups of order n. First write down a unique factorization for n:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

(p_i distinct).

For each term p^n in the factorization, consider all possible ways to write n as a sum of integers $n = m_1 + \cdots + m_s$. (These are called the partitions of n.)

Then the possible groups corresponding to p^n are

$$\mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_s}}.$$

Example:
Suppose $n = p^3$. Then the possible finite abelian groups of order n are $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$, and $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Example:
Suppose $n = p^2q^2$ (p, q distinct). Then the possible finite abelian groups of order n are $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{q^2}$, $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{q^2}$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q$, $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q$.

Overview

Congratulations!

You have all made huge progress in abstract reasoning and writing!

Symmetry
dihedral groups

Analysis/Synthesis
subgroups, normal subgroups
quotient group or factor group
Knowing about $H \lhd G$, G/H tells you about G.
Center, Centralizer
external and internal direct products

Classification
Cyclic groups:
Fundamental Theorem of Cyclic Groups, classification of all possible orders of elements and how many there are
Order $2p$: cyclic or dihedral

Maps that Preserve Structure
homomorphism, kernels
isomorphism, automorphism
Dihedral group of the square as geometric group, permutation group, matrix group
How to show groups are isomorphic and not isomorphic

Representation of a Group
permutations, matrices
Orbit-Stabilizer Theorem

Big Theorems:

Lagrange's Theorem:
$H < G$ implies $|H|$ divides $|G|$.

The First Isomorphism Theorem:
$G/(\text{Ker}\,\phi) \approx \phi(G)$.

Sylow's Theorem:
$p^k||G|$ implies G has a subgroup of order p^k.
Cauchy's Theorem:
$p||G|$ implies G has an element of order p.

Fundamental Theorem of Finite Abelian Groups

Evaluations

Mixing use of screen and board?

Pace of slides?

Covering homework in class (not enough? too much?)

Could you get enough help from me? (homework hints, accessible outside class)

Exam preparations

Discussion Board

Suggestions for improvement?