MATH 817 Notes

JD Nir
jnir@huskers.unl.edu
www.math.unl.edu/∼jnir2/817.html
October 20, 2015

Exam Tuesday:

- $\frac{1}{2}$ will be taken from list of 12 problems (do 2 of 3 that I list)
- $\frac{1}{2}$ will be new

We can devote Monday to review.

Def An automorphism of a group G is an isomorphism from G to G.

$\mathrm{Aut}(G)$ = the set of all automorphisms of G.

Lemma $\mathrm{Aut}(G) \leq \mathrm{Perm}(G)$

Pf Easy.

If G and N are groups, an action of G on N (as a set) is given by a group homomorphism $\rho : G \to \mathrm{Perm}(N)$.

If $\mathrm{im}(\rho) \subseteq \mathrm{Aut}(N) \leq \mathrm{Perm}(N)$ we say G acts on N via automorphisms.

Explicitly,

$$\text{action of } G \text{ on } N \text{ via automorphism} \quad \left\{ \begin{array}{l} \left.\begin{array}{l} (1)\ g' \cdot (g \cdot n) = (g'g) \cdot n \\ (2)\ e \cdot n = n \end{array}\right\} \text{action of } G \text{ on } N \text{ (as a set)} \\ (3)\ g \cdot (nn') = (g \cdot n)(g \cdot n')\ \forall g \in G, n, n' \in N \\ \qquad \uparrow \text{ product in } N \nearrow \end{array} \right.$$

Better notation: $n^g = g \cdot n$

(1) $(n^g)^{g'} = n^{g'g}$ $\quad (n^g)^{g'} = g' \cdot (g \cdot n) = (g'g) \cdot n = n^{g'g}$

(2) $n^e = n$

(3) $(nn')^g = (n^g)(n'^g)$

Main Example Assume $N \trianglelefteq G$. Then G acts on N via conjugation:

$\forall n \in N, g \in G$, $n^g := gng^{-1} \in N$ (since $N \trianglelefteq G$)

- $(n^g)^{g'} = (gng^{-1})^{g'} = g'gng^{-1}(g')^{-1} = g'gn(g'g)^{-1} = n^{g'g}$ ✓
- $n^e = ene^{-1} = n$ ✓
- $(nn')^g = gnn'g^{-1} = gng^{-1}gn'g^{-1} = n^g(n')^g$ ✓

So, the conjugation action of G on N is an action via automorphisms.

$\therefore$ We get a homomorphism $\rho : G \to \mathrm{Aut}(N)$

You can write it as $\rho(g) = \varphi_g$, where $\varphi_g \in \mathrm{Aut}(N)$ is defined by $\varphi)g(n) = n^g = gng^{-1}$

Examples: $n \neq 0$ $\mathrm{Aut}(\mathbb{Z}/n) \overset{(1)}{\cong} (\mathbb{Z}/n)^\times$

where $(\mathbb{Z}/n)^\times = (\{\overline{\ell} \mid \ell \in \mathbb{Z}, \gcd(\ell, n) = 1\}, \cdot)$

($\overline{\ell}$ = class mod n)

Proof of (1): Define $\Theta : (\mathbb{Z}/n)^\times \to \mathrm{Aut}(\mathbb{Z}/n)$ by

$$\Theta(\overline{\ell}) = \mu_{\overline{\ell}}, \text{ where } \mu_{\overline{\ell}} : \mathbb{Z}/n \to \mathbb{Z}/n$$

is $\mu_{\overline{\ell}}(\overline{m}) = \overline{\ell} \cdot \overline{m} = \overline{\ell m}$

To check:

- $\Theta(\overline{\ell})$ is independent of representation.
- $\mu_{\overline{\ell}}$ really is an automorphism of $\mathbb{Z}/n$ (uses $\gcd(\ell, n) = 1$)
- Θ is a homomorphism of groups: $\Theta(\overline{\ell}_1\overline{\ell}_2) = \Theta(\overline{\ell}_1) \circ \Theta(\overline{\ell}_2)$
  $\Leftrightarrow \mu_{\overline{\ell}_1} \circ \mu_{\overline{\ell}_2} = \mu_{\overline{\ell_1\ell_2}} : \overline{\ell}_1 \cdot (\overline{\ell}_2 \cdot \overline{m}) = \overline{\ell_1 \cdot \ell_2} \cdot \overline{m}$ ✓
- Θ is 1-1: $\Theta(\overline{\ell}_1) = \Theta(\overline{\ell}_2) \Rightarrow \mu_{\overline{\ell}_1} = \mu_{\overline{\ell}_2} \Rightarrow \overline{\ell}_1 \cdot \overline{1} = \overline{\ell}_2 \cdot \overline{1} \in \mathbb{Z}/n$
  $\Rightarrow \overline{\ell}_1 = \overline{\ell}_2 \in \mathbb{Z}/n$
  $\Rightarrow \overline{\ell}_1 = \overline{\ell}_2 \in (\mathbb{Z}/n)^\times$
- Θ is onto: If $\alpha \in \mathrm{Aut}(\mathbb{Z}/n)$, I need to show $\alpha = \mu_{\overline{\ell}}$, some $\overline{\ell}$. Let $\overline{\ell} = \alpha(\overline{1})$. If $0 \le m \le n-1$, then $\alpha(\overline{m}) = \alpha\left(\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{m}\right) = \underbrace{\alpha(\overline{1} + \cdots + \alpha(\overline{1})}_{m} = \overbrace{\overline{\ell} + \cdots + \overline{\ell}}^{m} = \overline{\ell \cdot m} = \mu_{\overline{\ell}}(\overline{m})$
  $\therefore\ \alpha = \mu_{\overline{\ell}}$.
  Finally, need to show $\gcd(\ell, n) = 1$. α is onto $\Rightarrow \mu_{\overline{\ell}}(\overline{m}) = \overline{1}$, some m.
  $\therefore\ \overline{\ell m} = \overline{1} \Rightarrow 1 = \ell m + an$, some a. □

Note $n \ge 2$ $\quad \begin{aligned} \#\,\mathrm{Aut}(\mathbb{Z}/n) &= \#\{\ell \mid 1 \le \ell \le n-1, \gcd(\ell, n) = 1\} \\ &= \varphi(n) \end{aligned}$

If p is prime then $\#\,\mathrm{Aut}(\mathbb{Z}/p) = p - 1$

Fact: If p is prime $(\mathbb{Z}/p)^\times$ is a cyclic group (of order $p-1$).

e.g. $(\mathbb{Z}/17)^\times$ is cyclic of order 16.

In fact $x = \overline{3}$ generates:

$\overline{3}$,	$\overline{9}$,	$\overline{10}$,	$\overline{13}$,	$\overline{5}$,	$\overline{15}$,	$\overline{11}$,	$\overline{16}$
x,	x^2,	x^3					x^8

$|x| \ge 9 \Rightarrow |x| = 16$

Application If $\#G = pq$, p and q are prime, and $p \le q$ and $p \nmid q - 1$, then G is abelian.

E.g. $\#G = 33 \Rightarrow G$ is abelian

Proof:

- If $p = q$, we already did this
- $p < q$.
  If $\#Z(G) = p$ or q, $G/Z(G)$ is cyclic $\Rightarrow G$ abelian $\Rightarrow\Leftarrow$
  It remains to prove $\#Z(G) = 1$ is impossible.

Claim $\exists x, y \in G$ such that $|x| = q$ and $|y| = p$. (True by Cauchy)

Let $H = \langle x \rangle$. $\#H = q$ $[G : H] = p$

$\therefore H \trianglelefteq G$.

$\therefore$ G acts on H via conjugation and this action is via automorphisms of H:

$\exists$ group homomorphism $\rho : G \to \mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}/q)$, $\#\,\mathrm{Aut}(H) = q - 1$.

$\#\,\mathrm{im}(\rho) \mid q - 1$ and $\#\,\mathrm{im}(\rho) \mid pq$

But $\gcd(q - 1, pq) = 1$

$\therefore$ $\#\,\mathrm{im}(\rho) = 1$

$\therefore$ $\forall g \in G, gxg^{-1} = x$. $y \in G \setminus H$

$G = \langle x, y \rangle$ and $xy = yx$.

$\therefore G$ is abelian.