Graduate Algebra, Fall 2014
Lecture 6

Andrei Jorza

2014-09-05

1 Group Theory

1.11 Automorphisms

Example 1. Have

1. $\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\}$.
2. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. In both cases $f \in \mathrm{Aut}(G)$ implies $f(k) = kf(1)$. For f to be surjective there must exist k such that $kf(1) = 1$ and so $f(1) = \pm 1$ in the first case and $f(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$ in the second case. If $kf(1) = 1$ for some k then f is in fact an automorphism with inverse f^{-1} taking 1 to k. Note that the map taking f to $f(1)$ is a homomorphism: indeed, $f(g(1)) = g(1)f(1)$ so we get the desired isomorphisms. □

Example 2. $\mathrm{Aut}(S_3) \cong S_3$.

Proof. Already $\mathrm{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$. Also, $S_3 = \langle (12), (123) \rangle$ and (12) can go to one of the three transpositions and (123) to one of the two 3-cycles. Thus the total number of automorphisms is at most $6 = |\mathrm{Inn}(S_3)|$ and so $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$. □

Proposition 3. *Suppose G and H are finite groups with coprime orders. Then* $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

Proof. Suppose $f \in \mathrm{Aut}(G \times H)$. Then restricting to $G \times 1$ and $1 \times H$ we get injections $f_G : G \to G \times H$ and $f_H : H \to G \times H$. Suppose $g \in G$ has order n. Then $f_G(a) = u \times v$ where $v \in H$. Since $a^n = 1$ it follows that $u^n = 1$ in G and $v^n = 1$ in H and so $\mathrm{ord}(v) \mid n, |H|$ so $\mathrm{ord}(v) = 1$ so $v = 1$. Thus we get $f_G : G \to G$ an injection which must then be a bijection. Get $f_G \in \mathrm{Aut}(G)$ and similarly $f_H \in \mathrm{Aut}(H)$. Finally, if $f \in \mathrm{Aut}(G)$ and $g \in \mathrm{Aut}(H)$ then $f \times g \in \mathrm{Aut}(G \times H)$ and so we get the desired isomorphism. □

Example 4. Let p and q be two primes. Then

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}) \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times & p \neq q \\ \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) & p = q \end{cases}$$

Proof. The case $p \neq q$ follows from the previous proposition. When $p = q$ the group $G = (\mathbb{Z}/p\mathbb{Z})^2$ is a two-dimensional vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and every group automorphism of G is also a vector space automorphism. Finally, vector space automorphisms are given by invertible matrices. □

1.12 Semidirect products

Proposition 5. *If $H, N \lhd G$ such that $H \cap N = 1$ and $G = HN$ then $G \cong H \times N$.*

Proof. Homework 3. $\square$

Proposition 6. *Let H, N be two groups and let $\phi : H \to \text{Aut}(N)$ be a homomorphism. Consider the set $G = H \times N$ together with the binary operation $(g, n) \cdot (h, m) = (gh, n\phi_g(m))$. Then*

1. *G is a group.*
2. *$N \lhd G$.*
3. *$H \cap N = 1$.*
4. *$G = HN$.*

The group G is said to be the semidirect product $G = N \rtimes_\phi H$ or simply $N \rtimes H$.

Proof. The binary operation is associative because ϕ is a homomorphism, $(1, 1)$ is a unit element and the inverse of (n, h) is $(\phi_{h^{-1}}(n^{-1}), h^{-1})$. The other statements are straightforward. $\square$

Proposition 7. *Let G be a group, H a subgroup and N a normal subgroup such that $G = NH$ and $H \cap N = 1$. Then for $h \in H$ get $\phi(h) \in \text{Aut}(N)$ given by $\phi(h, n) = hnh^{-1}$ and $G \cong N \rtimes_\phi H$.*

Proof. Since $G = NH$ every $g \in G$ is $g = nh$ for some $h \in H, n \in N$. Since $H \cap N = 1$ this expression is unique. Finally, if $g = nh$ and $g' = n'h'$ then $gg' = nhn'h' = nhn'h^{-1}hh' = n\phi(h, n')hh'$. $\square$

Example 8.

1. $D_{2n} \cong (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$ where $\phi : \mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ takes 0 to id and 1 to $x \mapsto -x$.
2. If $(n, \varphi(m)) = 1$ then $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Indeed, otherwise we need a homomorphism $\mathbb{Z}/n\mathbb{Z} \to \text{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and the order n element 1 in the LHS will have order dividing both n and the cardinality $\varphi(m)$ of the automorphism group. Thus is has order 1 and so ϕ is the trivial homomorphism.
3. $S_n \cong A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.
4. The identity morphism $(\mathbb{Z}/n\mathbb{Z})^\times \to \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ sending a to the multiplication by a automorphism yields the semidirect product

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times \cong \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z}\}$$