Graduate Algebra, Fall 2014
Lecture 4

Andrei Jorza

2014-09-03

1 Group Theory

1.7 Group quotients

For $g \in G$ and $H \subset G$ write $gH = \{gh|h \in H\}$ and $Hg = \{hg|h \in H\}$. If H and K are subsets then $HK = \{hk|h \in H, k \in K\}$.

Lemma 1. *Let $H \subset G$ be a subgroup. If $g, h \in G$ then gH and hH are either disjoint, if $g^{-1}h \notin H$, or coincide if $g^{-1}h \in H$. The same is true for Hg and Hh, depending on whether $gh^{-1} \in H$ or not.*

Proof. If $gx = hy$ for some $x, y \in H$ then $g^{-1}h = xy^{-1}$ so if $g^{-1}h \notin H$ then the two sets are disjoint. If $g^{-1}h = u \in H$ then $hH = guH = gH$ as $u \in H$. □

Definition 2. Define G/H as the set of cosets gH. Similarly write $H\backslash G$ for the set of cosets Hg.

Proposition 3. *Let $H \subset G$ be a subgroup.*

1. *The map $f(x) = x^{-1}$ gives a bijection $G/H \to H\backslash G$. The common cardinality $|G/H| = |H\backslash G|$ is denoted $[G : H]$.*
2. *If G is a finite group then $[G : H] = |G|/|H|$.*

Proof. For the first part: $(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$.

For the second part: the finite set G is partitioned into finitely many sets of cardinality $|H|$ and $|G/H|$ is the number of these sets. □

Corollary 4 (Lagrange)**.** *Let G be a finite group.*

1. *If H is a subgroup of G then $|H| \mid |G|$.*
2. *If $a \in G$ has order $\text{ord}(a) = m$ then $m \mid |G|$.*
3. *If $a \in G$ then $a^{|G|} = 1$.*

Proof. The first part follows from the proposition. The second from the fact that $|\langle a \rangle| = \text{ord}(a)$. The third part follows from the second part. □

Example 5.
1. For an integer n denote $\varphi(n)$ the cardinality of $(\mathbb{Z}/n\mathbb{Z})^\times$, the number of k between 1 and n coprime to n. Then for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ one has $a^{\varphi(n)} \equiv 1 \pmod{n}$. Indeed, $\text{ord}(a) \mid \varphi(n)$.
2. In particular, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.
3. If $|G| = p$ is a prime number then G is cyclic. Indeed, if $a \in G$ is nontrivial then $\text{ord}(a) \mid p$ and so $\text{ord}(a) = p$ and so $G = \langle a \rangle$.

Proposition 6. *From pset 2 if $K \subset H \subset G$ are subgroups then $[G : K] = [G : H][H : K]$ (with no finiteness assumption on G).*

1.8 Direct products

We already saw that if G and H are groups then $G \times H$ is a group, called the exterior direct product.

Definition 7. Suppose G is a group and $K, H \subset G$ are subgroups. The interior direct product of H and K is the **set** $HK = \{hk | h \in H, k \in K\} \subset G$.

Lemma 8. *The interior direct product HK is a subgroup of G if and only if $HK = KH$ as sets. Then $HK = \langle H \cup K \rangle$.*

Proof. If $HK = KH$ then any ratio of HK is still in HK and so HK is a subgroup. Reciprocally, if HK is a subgroup then $KH = (eK)(He) = (HK)(HK) = HK$. $\square$

Proposition 9.

1. *$[H : H \cap K] \leq [G : K]$*

2. *If $[G : K]$ is finite then $G = HK$ iff the above ineqality is in fact equality: $[H : H \cap K] = [G : K]$.*

Proof. Since $H \cap K \subset K$, $gH \cap K \subset gK$ and so we get a map $H/H \cap K \to G/K$ by sending the coset $gH \cap K$ to the unique coset gK containing it. Suppose that for $g, h \in H$, $gH \cap K$ and $hH \cap K$ are both sent to the same coset $gK = hK$. Then $g^{-1}h \in K$ but also in H and so in $H \cap K$ which means that $gH \cap K = hH \cap K$. Thus this map in injective proving the first part.

For the second part we need surjectivity since G/K has finite cardinality. Suppose $gK = hK$ for some $h \in H$. Then immediately $g \in hKK^{-1} = hK \subset HK$ and so surjectivity can only happen if $G = HK$. Suppose that $G = HK$. Then every $g \in G$ can be written $g = hk$ in which case $gK = hkK = hK$ and surjectivity follows. $\square$

1.9 Normal subgroups

Definition 10. A subgroup $H \subset G$ is said to be normal if $gHg^{-1} = H$ for every $g \in G$ in which case one writes $H \lhd G$.

Proposition 11. *If $H \lhd G$ then G/H and $H \backslash G$ become groups.*

Proof. Indeed, $gHhH = ghh^{-1}HhH = ghHH = ghH$ and $(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1} = g^{-1}gHg^{-1} = g^{-1}H$. $\square$

Lemma 12. *Suppose $f : G \to H$ is a homomorphism. Them $\ker f \lhd G$. Moreover, if $H \lhd G$ then $G \to G/H$ sending g to gH is a group homomorphism with kernel H.*

Proof. If $f(g) = 1$ and $h \in G$ then $f(hgh^{-1}) = f(h)f(g)f(h^{-1}) = f(h)f(h^{-1}) = 1$ and so $hgh^{-1} \in \ker f$. The second part is straightforward. $\square$

Example 13. General examples.

1. Every subgroup of an abelian group is normal.
2. If $H, K \lhd G$ then $H \cap K \lhd G$.
3. If $N \lhd G$ and N is a subgroup of a subgroup H of G then $N \lhd H$.
4. If $N \lhd G$ and H is a subgroup of G then $N \cap H \lhd H$.
5. If G is a group then $Z(G) \lhd G$.

Example 14. Specific examples.

1. The alternating group $A_n = \ker \varepsilon$ is a normal subgroup of S_n as ε is a homomorphism.
2. For $R = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, $\mathrm{SL}(n, R) \lhd \mathrm{GL}(n, R)$.

3. But $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\}$ is not normal in $\mathrm{GL}(2, R)$. Indeed, if $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ then $w \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} w = \begin{pmatrix} c & 0 \\ b & a \end{pmatrix}$.

4. But $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}$ is a normal subgroup of $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\}$.

Remark 1. If $H, K \subset G$ are subgroups such that K is normal in G then HK is a subgroup of G. Indeed, $KH = HK$.