16. Script zur Vorlesung: Algebra (B III)
Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller
WS 2016/2017: 20. Dezember 2016

1 Lagrange's theorem

Definition 1.1. *The **index** of a subgroup H in a group G, denoted $[G : H]$, is the number of left cosets of H in G ($[G : H]$ is a natural number or infinite).*

Theorem 1.2 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$ and*

$$[G : H] = \frac{|G|}{|H|}.$$

Proof. Recall that (see lecture 16) any pair of left cosets of H are either equal or disjoint. Thus, since G is finite, there exist $g_1, ..., g_n \in G$ such that

- $G = \cup_{i=1}^{n} g_i H$ and
- for all $1 \leq i < j \leq n$, $g_i H \cap g_j H = \emptyset$.

Since $n = [G : H]$, it is enough to now show that each coset of H has size $|H|$.
Suppose $g \in G$. The map $\varphi_g : H \to gH : h \mapsto gh$ is surjective by definition. The map φ_g is injective; for whenever

$$gh_1 = \varphi_g(h_1) = \varphi_g(h_2) = gh_2$$

, multiplying on the left by g^{-1}, we have that $h_1 = h_2$. Thus each coset of H in G has size $|H|$.
Thus

$$|G| = \sum_{i=1}^{n} |g_i H| = \sum_{i=1}^{n} |H| = [G : H]|H|$$

□

Note that in the above proof we could have just as easily worked with right cosets. Thus if G is a finite group and H is a subgroup of G then the number of left cosets is equal to the number of right cosets. More generally, the map $gH \mapsto Hg^{-1}$ is a bijection between the set of left cosets of H in G and the set of right cosets of H in G.

Corollary 1.3. *Let G be a finite group. For all $x \in G$, $|x|$ divides $|G|$. In particular, for all $x \in G$, $x^{|G|} = 1$.*

Proof. By Lagrange's theorem $|x| = |\langle x \rangle|$ divides $|G|$. $\square$

Corollary 1.4. *Every group of prime order is cyclic.*

Proof. Let G be a finite group with $|G|$ prime. Take $x \in G \backslash \{1\}$. By lagrange, $|x|$ divides G and thus, since $|G|$ is prime, $|x| = |G|$ or $|G| = 1$. Since $x \neq 1$, $|x| \neq 1$. Thus $|x| = |G|$ and so, $\langle x \rangle = G$. $\square$

Example: The converse of Lagrange's theorem does not hold. The group A_4 is of size 12 and has no subgroup of size 6. See exercise sheet 8 (Recall from linear algebra that A_4 is the group of all even permutations on 4 elements concretely: the set of permutations

$$(123), (132), (234), (243), (134), (143), (124), (142), (12)(34), (13)(24), (14)(23), e).$$

Definition 1.5. *Let G be a group and S, T subsets of G. We write*

$$ST := \{st \mid s \in S \text{ and } t \in T\}.$$

Proposition 1.6. *If K and H are subgroups of a finite group G then*

$$|HK||H \cap K| = |H||K|.$$

Proof. Let $\varphi : H \times K \to HK$ be the map defined by $\varphi(h, k) := hk$. This map is surjective by definition.

Claim: If $h \in H$ and $k \in K$ then $\varphi^{-1}(hk) = \{(hd^{-1}, dk) \mid d \in K \cap H\}$.

Clearly, if $d \in K \cap H$ and $h' = hd^{-1}, k' = dk$ then $h' \in H$, $k' \in K$ and $h'k' = hk$. Conversely, if $h' \in H$, $k' \in K$ and $h'k' = hk$ then $k'k^{-1} = h'^{-1}h \in K \cap H$, $h' = h(h'^{-1}h)^{-1}$ and $k' = (h'^{-1}h)k$. This proves the claim.

Therefore for each $x \in HK$, $|\varphi^{-1}(x)| = |H \cap K|$. So,

$$|HK||H \cap K| = |H \times K| = |H||K|.$$

$\square$

Proposition 1.7. *Let H and K be subgroups of a group G. The set HK is a subgroup of G if and only $HK = KH$.*

Proof. Suppose $h \in H$ and $k \in K$. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH$. Thus $g \in HK$ if and only if $g^{-1} \in KH$. So, if HK is a subgroup then $HK = KH$.
Suppose $HK = KH$. Take $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Consider $h_1k_1h_2k_2$. Since $k_1h_2 \in KH = HK$, there exist $h_3 \in H$ and $k_3 \in K$ such that $k_1h_2 = h_3k_3$. Thus $h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 \in HK$. So HK is closed under multiplication.
From above we know that if $g \in HK$ then $g^{-1} \in KH = HK$. Thus, since HK is non-empty, it is a subgroup of G. $\square$

Definition 1.8. *Let G be a group and A a subgroup of G. The normaliser, $N_G(A)$, of A in G is the set of $x \in G$ such that $xAx^{-1} = A$.*

Remark 1.9. *Let $A \leq B \leq G$ be groups. Note that $N_G(A)$ is a subgroup of G containing A; in fact, it is the largest subgroup of G in which A is normal.*

The subgroup A is normal in B if and only if $B \leq N_G(A)$. In particular, A is normal in G if and only if $N_G(A) = G$. (Please convince yourself that this is true)

Corollary 1.10. *If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.*

Proof. It is enough to show that $HK = KH$. Suppose that $h \in H$ and $k \in K$. Then $h^{-1}kh, hkh^{-1} \in K$ since $H \leq N_G(K)$. Thus $hk = (hkh^{-1})h \in KH$ and $kh = h(h^{-1}kh) \in HK$. Thus $HK = KH$. $\square$

2 Isomorphism theorems

Theorem 2.1. *If $\varphi : G \to H$ is a homomorphism of groups, then $ker\varphi \trianglelefteq G$ and*

$$G/ker\varphi \cong im\varphi.$$

Proof. We have already seen that the kernel of a homomorphism of groups is normal.
Define $f : G/\ker\varphi \to H$ by $f(a\ker\varphi) = \varphi(a)$.
This map is well-defined since: if $a\ker\varphi = b\ker\varphi$ then $ab^{-1} \in \ker\varphi$. So $1 = \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$. Thus $\varphi(a) = \varphi(b)$.
The map f is a homomorphism since:

$$f(a\ker\varphi b\ker\varphi) = f(ab\ker\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = f(a\ker\varphi)f(b\ker\varphi).$$

The image of f is clearly equal to the image of φ. Lastly, f is injective for if $f(a\ker\varphi) = f(b\ker\varphi)$ then $\varphi(a) = \varphi(b)$ and so $\varphi(ab^{-1}) \in \ker\varphi$ i.e. $a\ker\varphi = b\ker\varphi$.
Thus f gives a bijective group homomorphism from $G/\ker\varphi$ to $\mathrm{im}\varphi$. □

Corollary 2.2. *Let $\varphi : G \to H$ be a homomorphism of groups.*

1. *φ is injective if and only if $\ker\varphi = 1$*
2. *$[G : \ker] = |\varphi(G)|$*

Proof. (1) The forward direction follows directly from the definition of injective. Suppose $\ker\varphi = 1$ and $\varphi(a) = \varphi(b)$. Then $\varphi(ab^{-1}) = 1$. So $ab^{-1} = 1$ and thus $a = b$.
(2) $|G : \ker\varphi| = |G/\ker\varphi| = |\varphi(G)|$. □

Theorem 2.3 (The second isomorphism theorem). *Let G be a group and let A and B be subgroups of G with $A \le N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.*

Proof. Since $A \le N_G(B)$, AB is a subgroup of G. Since $B \le N_G(B)$, $AB \le N_G(B)$; that is B is normal in AB.
Consider the canonical projection $\pi : AB \to AB/B$. If $a \in A$ and $\pi(a) = 1$ then $a \in B$. Thus $a \in A \cap B$. So π restricted to A has kernel $A \cap B$ (and thus is normal). Now suppose $a \in A$ and $b \in B$. We have that $\pi(a) = \pi(ab)$. Thus π restricted to A is surjective i.e. $\mathrm{im}\pi|_A = AB/B$. So by first iso theorem $AB/B \cong A/A \cap B$. □

Theorem 2.4 (The third isomorphism theorem)**.** *Let G be a group and let H and K be normal subgroups with $H \leq K$. Then $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \cong G/K.$$

Proof. Consider the map $f : G/H \to G/K$ defined by $f(gH) = gK$. This map is well defined: If $g_1H = g_2H$ then $g_1^{-1}g_2 \in H$ and thus $g_1^{-1}g_2 \in K$. So $g_1K = g_2K$.
This map is a group homomorphism since

$$f(aHbH) = f(abH) = abK = aKbK = f(aH)f(bH).$$

It is clearly surjective. Suppose $a \in G$. Then $f(aH) = 1K$ if only if $aK = 1K$; that is if and only if $a \in K$. Thus K/H is the kernel of f and so K/H is normal in G/H and

$$(G/H)/(K/H) \cong G/K$$

$\square$