Group Theory

Emre Özer

Autumn 2019

Notes based on lectures by Vitali Averbukh.

Contents

1 Abstract Group Theory

1.1 Basics

Definition (Group)**.** A *group* is a *set* G with a *binary operation* $*$, where $* : G \times G \to G$, that satisfies the following axioms:

1. *(Closure - assumed)* By the definition of the binary operation (multiplication) $*$, we assume that G is closed under multiplication. Formally, $\forall a, b \in G$, we have $a * b = c \in G$.
2. *(Associativity)* The multiplication is associative: $\forall a, b, c \in G$, we have $a*(b*c) = (a*b)*c$.
3. *(Identity)* $\exists$ an identity $e \in G$ such that $\forall a \in G$, we have $e * a = a * e = a$.
4. *(Inverse)* $\forall a \in G$, $\exists$ an inverse $a^{-1} \in G$ such that $a * a^{-1} = e$.

Definition (Abelian group)**.** A group is said to be *abelian* if it is commutative, meaning $\forall a, b \in G$, we have $a * b = b * a$.

Proposition (Uniqueness of identity)**.** The identity in any group is unique.

Proof. Let e and e' be identities of the group G. Then, we have

$$e = e * e' = e'. \quad \square$$

Proposition (Left and right inverse)**.** The left inverse of any element in a group is identical to its right inverse.

Proof. Let a^{-1} be the right inverse of some $a \in G$. We have

$$a * a^{-1} = e \Rightarrow a^{-1} = a^{-1} * e = a^{-1} * (a * a^{-1}) = (a^{-1} * a) * a^{-1}$$
$$\Rightarrow (a^{-1} * a) = e. \quad \square$$

Proposition (Uniqueness of inverse)**.** The inverse of any element in a group is unique.

Proof. Suppose for some $a \in G$, there exists two inverses $b, c \in G$. Then, we have

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c. \quad \square$$

Proposition. Given two elements $a, b \in G$, we have

$$c = a * b \Rightarrow c^{-1} = b^{-1} * a^{-1}.$$

Proof.

$$c * c^{-1} = (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * a^{-1} = e. \quad \square$$

Note (Notation)**.** From now on, when it is obvious we are referring to a single multiplication, we will omit $*$.

Theorem (Rearrangement)**.** Let $g_1, g_2, \ldots, g_n \in G$ be a finite group. Choose an element $g_i \in G$ and construct a new set $g_1 g_i, g_2 g_i, \ldots, g_n g_i \in G'$. Then, G' is a group and in fact, the same group as G.

Proof. Consider an element $a \in G$. We have $a = a g_i^{-1} g_i$. Since we know $g_i^{-1} \in G \Rightarrow a g_i^{-1} \in G$. So, $a = b g_i$ for some $b = a g_i^{-1} \in G$. Hence, $a \in G'$ $\forall a \in G$ since a was arbitrary. We know there are n elements in G' by construction. So, all elements appear without any new elements and so $G = G'$. $\square$

Definition (Cyclic group)**.** A group G is *cyclic* if $\exists a \in G$ and $\exists n \in \mathbb{Z}$, such that $\forall b \in G$, $b = a^n$. In such a group, a is called the *generator* of the group.

Note (Notation)**.** $\langle a \rangle$ denotes the cyclic group generated by a.

Definition (Order of an element)**.** The *order* $n \in \mathbb{Z}$ of an element $a \in G$ is the smallest integer such that $a^n = e$.

1.2 Subgroups

Definition (Subgroup)**.** $H \subseteq G$ is a *subgroup* if it forms a group with the same binary operation $*$ as G. We denote the subgroup $H \leq G$.

Proposition. A subset $H \subset G$ is a subgroup if and only if for all $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.

Proof. ($\Rightarrow$) Let $H \leq G$. Then, H must be closed so for all $h_1, h_2 \in H$, $h_1 h_2 \in H$. H must also contain inverses, so for all $h_1 \in H$, $h_1^{-1} \in H$. So, we may let $h_2 \to h_2^{-1}$ and combine the two statements into $h_1 h_2^{-1} \in H$. If we let $h_2 = h_1$, we obtain $h_1 h_1^{-1} = e \in H$. And letting $h_1 = e$ we obtain the inverse axiom $h_2^{-1} \in H$ for all h_2.

($\Leftarrow$) Simply look at the axioms. Identity exists, let $h_2 = h_1$. Inverses exist, let $h_1 = e$. H is closed, let $h_2 \to h_2^{-1}$. □

Proposition. The cycle of any element $g \in G$ is a subgroup.

Proof. For closure, note that $\forall k_1, k_2 \in \mathbb{Z}$, $g^{k_1}, g^{k_2} \in \langle g \rangle$. Then,

$$g^{k_1} g^{k_2} = g^{k_1 + k_2} = g^{k_3} \in \langle g \rangle .$$

Let h be the order of g, then we have identity

$$g^h = e \in \langle g \rangle .$$

We also have inverses, for any integer k

$$g^{h-k} g^k = g^h = e \Rightarrow g^{h-k} = \left(g^k\right)^{-1} \in \langle g \rangle .$$

Associativity is inherited from G, hence $\langle g \rangle$ is a group. □

Proposition. Cycles are abelian.

Proof. For any two integers k and ℓ, we have for $\langle g \rangle$ that

$$g^k g^\ell = g^{k+\ell} = g^\ell g^k. \quad \square$$

Definition (Centre)**.** For a given group G, the *centre* $Z(G)$ is the set of elements which commute with all elements of G,

$$Z(G) = \{h \in G : gh = hg \text{ for all } g \in G\}.$$

1.3 Cosets and Lagrange's theorem

Definition (Coset)**.** Let $H \leq G$ and $a \in G$. Then the set $aH = \{ah : h \in H\}$ is a *left coset of* H and the set $Ha = \{ha : h \in H\}$ is a *right coset of* H.

Proposition. A coset gH is a subgroup if and only if $g \in H$, in which case $gH = H$.

Proof. ($\Rightarrow$) Assume gH is a subgroup, so $e \in gH \Rightarrow g^{-1} \in H$. Then, by the inverse axiom, $g \in H$.

($\Leftarrow$) If $g \in H$, $gH = H$ by the rearrangement theorem. Since H is a subgroup, so is gH. □

Proposition. All cosets have the same number of elements.

Proof. Each left coset of H, denoted aH for some $a \in G$, must have the same number of elements since there exists a bijection between them. Let aH and bH be two cosets, then $\phi : aH \to bH$ is a bijection, where $\phi(h) = ba^{-1}$. The same argument follows for right cosets. □

Proposition. Two cosets aH and bH are either *equal* or *disjoint*.

Proof. Consider two *distinct* cosets aH and bH and suppose for some $h_1, h_2 \in H$, we have $ah_1 = bh_2 \in aH, bH$ (the two cosets share at least one element). Then, we have

$$ah_1 = bh_2 \Rightarrow a = bh_2h_1^{-1} = bh_3 \quad \text{for some} \quad h_3 \in H.$$

Then, for all $ah \in aH$, we have $ah = b(h_3h) \in bH \Rightarrow aH = bH$. But we assumed aH and bH were distinct, hence we conclude that they cannot share any elements.

Definition (Partition)**.** Let X be a set, and $X_1, X_2, \ldots X_n \subseteq X$. The X_i are called a *partition* of X if $\bigcup X_i = X$ and $X_i \cap X_j = \emptyset$ for all $i \neq j$.

Proposition. The left cosets of $H \leq G$ partition G.

Proof. We've already proved that distinct cosets do not intersect. Now, we just need to prove that the union of all left cosets equals G. Since $e \in H$, the set $\bigcup aH = \{ah : a \in G, h \in H\} = G$. This is obvious, just set $h = e$. The proposition follows. □

Theorem (Lagrange's theorem)**.** Let G be a finite group with $H \leq G$. Then, $|H|$ divides $|G|$. We may denote

$$\frac{|G|}{|H|} = |G : H| \in \mathbb{Z}.$$

Proof. We've already proved the necessary propositions. Putting everything together: suppose there are $|G : H|$ left cosets of H, each with size $|H|$. Since they partition the group G, we have

$$|G : H||H| = |G|. \quad \square$$

1.4 Conjugates, normal subgroups

Definition (Equivalence relation)**.** A *binary relation* $\sim: X \times X \to X$ on a set X is said to be an *equivalence relation* if and only if for all $a, b, c \in X$ it is

1. reflexive: $a \sim a$,
2. symmetric: $a \sim b \Leftrightarrow b \sim a$,
3. transitive: if $a \sim b$ and $b \sim c$, it follows $a \sim c$.

Definition (Equivalence class)**.** Given a set X and an equivalence relation $\sim$ on X, the *equivalence class* of an element $a \in X$, denoted $[a]$ is the set

$$[a] = \{x \in X : x \sim a\}.$$

Definition (Conjugate elements)**.** Two group elements g_1 and g_2 are called *conjugate*, written $g_1 \sim g_2$ if there exists $g \in G$ such that

$$g_1 = gg_2g^{-1}.$$

Proposition. Conjugacy is an equivalence relation.

Proof. Simply look at the conditions:

1. reflexive: $g_1 = gg_1g$ for all $g_1 \in G$ when $g = e$.
2. symmetric: let g_1 and g_2 be conjugates. Then $\exists g \in G$ such that

$$g_1 = gg_2g^{-1} \Rightarrow g_2 = g^{-1}g_1g$$

   where $g^{-1} \in G$.

3. For some $a, b \in G$ let $g_1 = ag_2a^{-1}$ and $g_2 = bg_3b^{-1}$. Then, it follows

$$g_1 = abg_3b^{-1}a^{-1} = (ab)g_3(ab)^{-1},$$

where $ab \in G$. This completes the proof. $\square$

Definition (Conjugacy class)**.** Since conjugacy is an equivalence relation, we can form equivalence classes, which we call *conjugacy classes*. So, we have

$$[g] = \{h \in G : h \sim g\}.$$

g is called the *representative* of the class.

Proposition. $g \sim g' \Leftrightarrow [g] = [g']$.

Proof. ($\Rightarrow$) By the transitive property, $g' \sim g$ implies g' is conjugate to all elements in $[g]$, so $[g] \subseteq [g']$. The same holds the other way around due to the symmetric property, so $[g'] \subseteq [g]$. Hence $[g] = [g']$.

($\Leftarrow$) Due to the reflexive property, $g \in [g]$. Since $[g] = [g']$, it follows $g \in [g']$ and so $g' \sim g$ as required. $\square$

Proposition. For Abelian groups, every element is its own conjugacy class.

Proof. Let G be an arbitrary group and assume $g_1 \sim g_2$. Then, for all $g \in G$ we have

$$g_1 = gg_2g^{-1} = (gg^{-1})g_2 = g_2.$$

Hence, $g_1 \sim g_2 \implies g_1 = g_2$ and so $[g_1] = \{g_1\}$. Since g_1 was arbitrary, this holds for all elements. $\square$

Proposition. The identity is always its own conjugacy class.

Proof. Assume for some $a \in G$ that $e \sim a$. Then,

$$a = geg^{-1} = gg^{-1} = g,$$

hence $a \sim e \Rightarrow a = e$ and so $[e] = \{e\}$. $\square$

Proposition. If g is of order p, every element of $[g]$ is also of order p.

Proof. Let $h \in [g]$. First, we show $h^p = e$. Then, we show $\nexists m < p$ such that $h^m = e$.

1. Since $h \sim g$, there exists $k \in G$ such that $h = kgk^{-1}$. It then follows that

$$h^p = \left(kgk^{-1}\right)^p = kg\underbrace{k^{-1}k}_{=e}gk^{-1}\dots kgk^{-1} = kg^pk^{-1} = kk^{-1} = e.$$

2. Assume $\exists m < p$ such that $h^m = e$. Then, by symmetry $g^m = e$ so g has order $m \neq p$. This is a contradiction, hence $\nexists m < p$ such that $h^m = e$.

Putting the two together we conclude $h \in [g]$ must also have order p. $\square$

Definition (Normal subgroup)**.** A subgroup $H \leq G$ is called a *normal (or invariant) subgroup* if it is self-conjugate, meaning

$$gHg^{-1} = H, \quad \text{for all} \quad g \in G.$$

This is denoted $H \lhd G$. An equivalent definition is that H is a normal subgroup if its left and right cosets are equal, $gH = Hg$ for all $g \in G$.

Proposition. A normal subgroup must be a union of conjugacy classes.

Proof. Suppose $H \lhd G$ and let $h \in H$. It is sufficient to show that $[h] \subseteq H$. So, consider some $k \in G$ such that $k \sim h$. So, there exists $g \in G$ such that $k = ghg^{-1}$. Since H is a normal subgroup, it then follows that $k \in H$. This holds for all $k \sim h$, therefore $[h] \subseteq H$. Since h was arbitrary, all elements in H must belong to a conjugacy class. □

Proposition. For Abelian groups, every subgroup is normal.

Proof. Almost trivially, $gHg^{-1} = gg^{-1}H = eH = H$. □

Proposition. The centre is always a normal subgroup.

Proof. Let $Z(G)$ be the centre of group G. Then, by construction, any $z \in Z(G)$ commutes with all $g \in G$. Hence,

$$(\forall z \in Z(G), g \in G), \quad gzg^{-1} = gg^{-1}z = z \in Z(G). \quad \square$$

Proposition. A subgroup which contains half of all elements, meaning $|G| = 2|H|$ is normal.

Proof. Assume $\exists g \in G$ such that $gHg^{-1} \neq H$. This implies $g \notin H$. Now, consider the cosets gH and Hg. Since H is assumed to be not normal, $gH \neq Hg$. But cosets partition the group, which implies that either $gH = H$ or $Hg = H$. In either case, it follows that $g \in H$ so we reach a contradiction and so H must be normal. □

Proposition. Let $N \leq H \leq G$, then $N \lhd G \Rightarrow N \lhd H$.

Proof. This is almost a trivial statement. Since $N \lhd G$, we have for all $g \in G$ that $gNg^{-1} = N$. Since $H \subseteq G$, the proposition follows. □

Definition (Simple group)**.** A group which has no nontrivial subgroups (i.e. other than $\{e\}$ and G itself) is called *simple*.

1.5 Quotient groups

Definition (Quotient group)**.** Let $H \lhd G$. The *quotient group* is the set of left cosets of H,

$$G/H = \{gH : g \in G\},$$

with the group operation defined as

$$g_1H \cdot g_2H = g_1g_2H.$$

Note (Quotient group in terms of group action)**.** The quotient group G/H is essentially the *right group action* of the *group* $H \lhd G$ on the *set* G. (See later section on group actions for more detail.)

Notice that there are group elements $g' \neq g$ for which $gH = g'H$. For the group operation to be well defined, we require that we get the same results by replacing $g \to g'$. We phrase this as follows:

Proposition. The group operator of G/H is well defined. Explicitly, for any $k, g \in G$, under a replacement $g \to g', k \to k'$ such that $gH = g'H$ and $kH = k'H$, the group operator gives the same result:

$$g'H \cdot k'H = g'k'H = gkH = gH \cdot kH.$$

Proof. We start by noting that $gH = g'H \Rightarrow g' = gh$ for some $h \in H$. This is easy to see, since $e \in H$ simply consider $g'e = g' \in gH$. Also, note that $hH = H$. So, we have

$$g'k'H = g'H \cdot k'H = ghH \cdot khH = ghH \cdot kH = ghkH = (gkk^{-1}g^{-1})ghkH = gkk^{-1}hkH.$$

Now, since H is a normal subgroup, we have for any $k \in G$, $k^{-1}hkH = H$, and so the result follows:

$$g'k'H = gkk^{-1}hkH = gkH. \quad \square$$

1.6 Group homomorphisms

Definition (Group homomorphism)**.** A *group homomorphism* is a map $f : G \to H$ between two groups $(G, \times), (H, *)$, which preserves the group structure. Explicitly,

$$\forall g_1, g_2 \in G, \quad f(g_1 \times g_2) = f(g_1) * f(g_2).$$

Definition (Group isomorphism)**.** A *group isomorphism* is a bijective homomorphism. Two groups are *isomorphic*, denoted $G \cong H$, if there exists an isomorphism between them.

Definition (Group automorphism)**.** A group isomorphism from a group to itself is a *group automorphism.*

Note. We will drop the "group" and denote "group homomorphism" by "homomorphism" from now on (and similar for isomorphisms).

Corollary. From the definition of homomorphisms, it directly follows that for any homomorphism $f : G \to H$ we have

- $\forall g \in G$, we have $f(g) = f(ge_G) = f(g)f(e_G) \Rightarrow f(e_G) = e_H$.
- $\forall g \in G$, $e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1}) \Rightarrow f(g^{-1}) = (f(g))^{-1}$.

Definition (Image)**.** The image of f, denoted $f(G)$, is the part of H reached by f:

$$f(G) = \{h \in H : \exists g \in G \text{ with } f(g) = h\}.$$

Definition (Kernel)**.** The kernel of f, denoted $\ker f$, is the subset of G mapped to the identity in H:

$$\ker f = \{g \in G : f(g) = e_H\}.$$

Proposition. f is injective if and only if $\ker f = \{e_G\}$.

Proof. ($\Rightarrow$) If f is injective, at most a single element in G may be mapped to e_H. Since $f(e_G) = e_H$, it follows that $\ker f = \{e_G\}$.

($\Leftarrow$) Suppose $\ker f = \{e_G\}$ and f is not injective. Then, $\exists g \neq h$ in G such that $f(g) = f(h) \Rightarrow f(g^{-1}h) = e_H$, and so $g^{-1}h \in \ker f$. This is a contradiction, so f must be injective. $\square$

Note. From now on we also drop the G and H subscripts from the identity.

Theorem (Isomorphism theorems)**.** There are three important theorems:

1. Let $f : G \to H$ be a group homomorphism. Then, we have the following properties:

   (a) The kernel $\ker f$ is a normal subgroup of G, $\ker f \lhd G$.

   Proof. For any $g \in G$, we have

   $$f\big(g \ker f g^{-1}\big) = f(g)f(\ker f)f(g^{-1}) = f(g)f(g^{-1}) = e \in \ker f.$$

   $\square$

(b) The image $f(G)$ is a subgroup of H, $f(G) \leq H$.

Proof. Let $h_1, h_2 \in f(G)$, so there exists $g_1, g_2 \in G$ such that $h_1 = f(g_1)$ and $h_2 = f(g_2)$. Now, consider $h_1 h_2^{-1}$,

$$h_1 h_2^{-1} = f(g_1) f(g_2^{-1}) = f(g_1 g_2^{-1}) \in f(G),$$

since $g_1 g_2^{-1} \in G$. $\square$

(c) The quotient $G/\ker f$ is isomorphic to $f(G)$ with the isomorphism:

$$\widetilde{f} : G/\ker f \to f(G), \quad \widetilde{f}(g \ker f) = f(g).$$

Proof. $\widetilde{f}$ is surjective by construction, we just need to prove injectivity. So, consider the kernel of $\widetilde{f}$. Suppose $g \ker f$ is mapped to the identity e so that $g \ker f \in \ker \widetilde{f}$. Then, we have $f(g) = e \Rightarrow g \in \ker f$. Hence, we conclude $g \ker f = \ker f$, which is the identity element of $\widetilde{f}$. Hence, $\widetilde{f}$ is injective and therefore an isomorphism. $\square$

2. Let $H \leq G$ and $N \lhd G$. Then, we have

(a) The product HN is a subgroup of G, where $HN = \{hn : h \in H, n \in N\}$.

Direct proof. Let $h_1 n_1$ and $h_2 n_2$ be arbitrary elements in HN. Consider $h_1 n_1 (h_2 n_2)^{-1}$,

$$h_1 n_1 (h_2 n_2)^{-1} = h_1 \underbrace{n_1 n_2^{-1}}_{\equiv n_3 \in N} h_2^{-1} = h_1 h_2 h_2^{-1} h_1^{-1} h_1 n_3 h_2 = \underbrace{h_1 h_2}_{h_3 \in H} \underbrace{h_2^{-1} n_3 h_2}_{n_4 \in N} = h_3 n_4 \in HN.$$

$\square$

Homomorphism proof. Alternatively, we may use theorem 1.(b) and construct the trivial homomorphism $f : HN \to G$ with $f(hn) = hn$. Then, it follows that $HN \leq G$ provided HN is a group. $\square$

(b) The intersection $H \cap N$ is a normal subgroup of H.

Direct proof. Let $n \in H \cap N$. Then, for all $h \in H$ we have

$$hnh^{-1} \in N$$

since $N \lhd G \geq H$, so if $H \cap N \leq H$, then it is normal. We can show $H \cap N \leq H$ almost trivially, consider $n_1, n_2 \in H \cap N$. Then $n_1 n_2^{-1} \in H \cap N$ since both elements are in N and H. So, $H \cap N \lhd H$. $\square$

Homomorphism proof. We construct a homomorphism f, from H, with kernel $H \cap N$. Then, by 1.(a) the proposition follows. So, consider $f : H \to H/N$ with $f(h) = hN$. The identity in H/N is $N = nN$ for any $n \in N$. So, for any $n \in H \cap N$ we have $f(n) = nN = N$ and so the kernel $\ker f = H \cap N$. Finally, f is a homomorphism because it preserves the group structure, in particular consider for any $h \in H$ and $n \in H \cap N$,

$$f(h) = f(n) f(h) = f(nh) = nhN = hh^{-1} nhN = hN.$$

$\square$

(c) There is an isomorphism of the quotient groups,

$$HN/N \cong H/(H \cap N).$$

Proof. First, note that $HN/N = H/N$, since for any $hnN \in HN/N$, we have $hnN = hN \in H/N$. Since $H \subseteq HN$, it follows that there exists a trivial bijection. Now, we use theorem 1.(c) and consider a bijection $f : H \to H/N$ with $f(h) = hN$. As previously shown, the kernel is $\ker f = H \cap N$. The image is the set

$$f(H) = \{hN : h \in H\} = H/N = HN/N.$$

So, f is a homomophism with $f(H) = HN/N$ and $\ker f = H \cap N$. The proposition follows by 1.(c). □

3. Let H and N be normal subgroups of G, and let $N \leq H$. Then, $N \lhd H$ (already proved), and

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

Proof. Consider the map $f : G/N \to G/H$, with $f(gN) = gH$. This is well defined because if $g'N = gN$, then $g' = gn$ for some $n \in N$. And since $N \subset H$, we have $n \in H$ and so $gH = g'H$.

Map f is a homomorphism since for any $gN, g'N \in G/N$,

$$f(gN)f(g'N) = f(gN \cdot g'N) = f(gg'N) = gg'H = gH \cdot g'H.$$

The image $f(G)$ is obviously G/H. The kernel is given by all $gN \in G/N$ such that

$$gN = H = hH$$

for some $h \in H$. So, we conclude that $g \in H$, and so $\ker f \in H/N$. □

1.7 Product groups

Definition (Direct product)**.** Given two groups $G_{1,2}$, the *direct product* is the set

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}.$$

This defines a group under the group product

$$(g_1, g_2) \cdot (g_1' g_2') = (g_1 g_1', g_2 g_2').$$

This generalizes to finitely many group factors $G_1 \times \ldots \times G_n$.

Proposition. $G_1 \times G_2$ has normal subgroups $(G_1, e) \cong G_1$ and $(e, G_2) \cong G_2$.

Proof. The isomorphisms are obvious, $(g_1, e) \longmapsto g_1$ and $(e, g_2) \longmapsto g_2$. The groups are normal, since for all $(g_1', g_2') \in G_1 \times G_2$, we have

$$(g_1', g_2') \cdot (G_1, e) \cdot (g_1'^{-1}, g_2'^{-1}) = (g_1' G_1, g_1'^{-1}, g_2' e g_2'^{-1}) = (G_1, e),$$

and similarly for (e, G_2). In fact, we may go further and say that for any $z_1 \in Z(G_1)$ and $z_2 \in Z(G_2)$, we have $(G_1, z_2) \lhd (G_1 \times G_2)$ and $(z_1, G_2) \lhd (G_1 \times G_2)$. □

Proposition. There are natural group homomorphisms (projections) $\pi_{1,2} : G_1 \times G_2 \to G_{1,2}$, and every element in $G_1 \times G_2$ is uniquely given in terms of $(g_1, g_2) = (g_1, e) \cdot (e, g_2)$.

Proposition. Suppose G is a group with subgroups H and K such that

1. H and K are normal in G,
2. $H \cap K = \{e\}$,

3. They generate the group, meaning $G = HK$.

Then $G \cong H \times K$.

Proof. We start by noting that 1 and 2 imply $hk = kh$ for any $h \in H$ and $k \in K$. This is simply due to $k^{-1}hkh^{-1} \in H \cap K$ and so $k^{-1}hkh^{-1} = e$ hence $hk = kh$.

Now consider the map $f : H \times K \to G$, with $(h, k) \longmapsto hk$. This is well defined, to see why suppose $h'k' = hk$ for some $h, h' \in H$ and $k, k' \in K$. Then,

$$h'k' = hk \Rightarrow h'^{-1}h = k'k^{-1} = e \Rightarrow h = h' \quad \text{and} \quad k = k',$$

where we used condition 2. The map f is a homomorphism, since

$$(h, k) \cdot (h', k') = (hh', kk') \longmapsto hh'kk' = hkh'k' = (hk)(h'k').$$

By condition 3, f is surjective. To prove injectivity, note that

$$\ker f = \{hk = e : h \in H, k \in K\} \Rightarrow h = k^{-1} \Rightarrow h, k \in H \cap K \Rightarrow h = k = e.$$

Hence, $\ker f = \{(e, e)\}$ and so f is injective. So, f is bijective. □

Definition (Semidirect product)**.** Given two groups H and N and a homomorphism $\theta : H \to \operatorname{Aut} N$, the *semidirect product* is defined as the group

$$G \cong N \rtimes H = \{(n, h) : n \in N, h \in H\},$$

with the group product defined as

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\theta(h_1)n_2, h_1h_2).$$

Proposition. G is (isomorphic to) the semidirect product if its subgroups N and H if

1. N is a normal subgroup of G,
2. $N \cap H = \{e\}$,
3. $G = NH$, so N and H generate group G.

Note that the only difference between the direct product is the first condition, where we don't require H to be normal.

2 Representation Theory

2.1 Group actions

Definition (Left group action)**.** Let G be group and X be a set. Then, a *left group action* φ of G on X is a function

$$\varphi : G \times X \to X, \quad (g, x) \mapsto \varphi(g, x) = g \cdot x$$

which satisfies the axioms:

- *Identity:* $\forall x \in X, \varphi(e, x) = x$.
- *Compatibility:* $\forall g, h \in G, x \in X, \varphi(gh, x) = \varphi(g, \varphi(h, x))$.

From these axioms, it follows that for every $g \in G$, the function which maps $x \mapsto \varphi(g, x)$ is a bijection, with inverse $x \mapsto \varphi(g^{-1}, x)$.

Definition (Symmetric group)**.** The *symmetric group* of a finite set X, denoted $\operatorname{Sym} X$, is the set of all bijections $f : X \to X$ with group operation of function composition.

Corollary. Since every $\varphi(g, x)$ is a bijection, it is in the symmetric group of X. Consider the map

$$\theta : G \to \operatorname{Sym} X, \quad g \mapsto \varphi(g, \cdot).$$

By the compatibility axiom, θ is a group homomorphism. Conversely, every such homomorphism defines a group action of G on X.

Definition (Right group action)**.** Let G be group and X be a set. Then, a *right group action* φ of G on X is a function

$$\varphi : G \times X \to X, \quad (x, g) \mapsto \varphi(x, g) = x \cdot g$$

which satisfies the axioms:

- *Identity:* $\forall x \in X, \varphi(x, e) = x$.
- *Compatibility:* $\forall g, h \in G, x \in X, \varphi(x, gh) = \varphi(\varphi(x, g), h)$.

Note (Notation)**.** We denote $\varphi(g, x) = g \cdot x$ and $\varphi(x, g) = x \cdot g$.

Definition. Some natural definitions:

- An action is *faithful* if the kernel of the homomorphism $\theta : G \to \operatorname{Sym} X$ is $\{e\}$, so different group elements are assigned different maps.
- An action is *transitive* if $\forall x, y \in X, \exists g \in G$ such that $g \cdot x = y$.
- Given $g \in G$ and $x \in X$, x is a *fixed point of* g if $g \cdot x = x$.
- For an $x \in X$, the *stabilizer subgroup* of G is the set of all elements in G that fix x:

  $$G_x = \{g \in G : g \cdot x = x\}.$$

- A group action is said to be *free* if the stabilizer subgroup G_x for all x is trivial, meaning

  $$\forall x \in G, \quad G_x = \{e\}.$$

- If a group action is both transitive and free, it is *regular*.

- Given a point $x \in X$, its *orbit* is the set of all images of x under action of g:

$$Gx = \{g \cdot x : g \in G\}.$$

Theorem (Stabiliser-orbit)**.** For any given $x \in X$, the orbit Gx is in one-to-one correspondence with the set of left cosets of the stabiliser of x, with the map $g \cdot x \longmapsto gG_x$.

Proof. We simply need to prove that for any $g_1, g_2 \in G$,

$$g_1 \cdot x = g_2 \cdot x \Longleftrightarrow g_1 G_x = g_2 G_x.$$

($\Rightarrow$) Suppose $g_1 \cdot x = g_2 \cdot x$. Then, we have $g_1 \cdot x = g_2 \cdot (g_2^{-1} g_1 \cdot x)$. This implies that $g_2^{-1} g_1 \in G_x$, hence we have

$$g_2 G_x = g_2 \big(g_2^{-1} g_1 G_x\big) = g_1 G_x.$$

($\Leftarrow$) By the same procedure, $g_1 G_x = g_2 G_x$ implies $g_2^{-1} g_1 \in G_x$ from which it follows that $g_1 \cdot x = g_2 \cdot x$. ☐

2.2 Representations

Definition (General linear group)**.** Let V be a vector space over the field F. The general linear group on V, written GL(V) or $\operatorname{Aut} V$, is the group of all *automorphisms* of V, i.e. the set of all *bijective linear transformations* $V \to V$ together with functional composition as group operation.

Definition (Representation)**.** A representation of a group G on a vector space V is *a group homomorphism* D from G to the general linear group on V,

$$D : G \longrightarrow \operatorname{Aut} V.$$

V is called the *representation space*, the dimension of the representation is the dimension of V.