

# Graduate Algebra

## Contents

1. Week 1 [2025-09-03]	2
1.1. Notations and recollections	2
1.2. Groups	2
1.3. Rings	3
1.4. Fields	3
1.5. Linear Algebra	3
1.6. Cayley's Theorem	4
1.7. A linear analogue of Cayley's Theorem.	5
2. Week 2 [2025-09-08]	7
2.1. The Quotient of a set by an equivalence relation	7
2.2. Sub-groups	9
2.3. Group actions	10
2.4. Quotients of groups	11
2.5. Quotients of groups and orbits.	13
2.6. The product of subgroups	14
2.7. Lagrange's Theorem	16
3. Week 3 [2025-09-15]	18
3.1. Normal subgroups	18
3.2. Quotient groups	20
3.3. First isomorphism theorem	22
3.4. Groups acting on Groups	22
3.5. $p$ -groups	23
3.6. Sylow subgroups	25

## 1. Week 1 [2025-09-03]

We'll begin by recalling some basic sorts of algebra that you more-or-less encountered before.

### 1.1. Notations and recollections

We reserve the following letters:

- $\mathbb{N}$  for the set of *natural numbers*  $0, 1, 2, \dots$
- $\mathbb{Z}$  for the set of *integers*, i.e. for all  $\pm n$  for  $n \in \mathbb{N}$
- $\mathbb{Q}$  for the set of *rational numbers*  $m/n$  for  $m, n \in \mathbb{Z}$  with  $n \neq 0$
- $\mathbb{R}$  for the set of *real numbers*, and
- $\mathbb{C}$  for the set of *complex numbers*  $a + bi$  for  $a, b \in \mathbb{R}$ .

In this first lecture, I want to recall some of the main objects of study in algebra, including: groups, rings and fields. Ultimately, the goal today is to prove an analogue of Cayley's Theorem - see [Theorem 1.6.1](#) and [Theorem 1.7.1](#) about embedding arbitrary groups in some standard groups.

### 1.2. Groups

Recall that a group is a set  $G$  together with a binary operation  $\cdot : G \times G \rightarrow G$  satisfying the following:

- associativity:  $\forall x, y, z \in G, (xy)z = x(yz)$
- identity:  $\exists e \in G, xe = ex = x$ .
- inverses:  $\forall x \in G, \exists y \in G, xy = yx = 1$ .

*Remark 1.2.1:*

- a. We usually write  $1$  or sometimes  $1_G$  rather than  $e$  for the identity element of  $G$ .
- b. we usually write  $x^{-1}$  for the inverse of  $x \in G$
- c. there are *uniqueness* results that I'm eliding here; the identity  $1$  of  $G$  is unique, and the inverse  $x^{-1}$  of an element is unique. These statements are *consequences* of the above axioms (they don't require additional assumption.)
- d. A group is abelian if  $\forall a, b \in G, ab = ba$
- e. Sometimes we write groups additively; in that case,  $0$  is the identity element and the inverse of  $a \in G$  is  $-a \in G$ . We always insist that additive groups are abelian.

**Definition 1.2.2:** For groups  $G$  and  $H$ , a function  $\varphi : G \rightarrow H$  is a **group homomorphism** provided that  $\forall x, y \in G, \varphi(xy) = \varphi(x)\varphi(y)$ .

**Definition 1.2.3:** Let  $\varphi : G \rightarrow H$  be a group homomorphism. The **kernel** of  $\varphi$  is

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1.\}$$

*Remark 1.2.4:* If  $\varphi : G \rightarrow H$  is a group homomorphism,  $\ker \varphi$  is a subgroup of  $G$  - i.e.  $\ker \varphi$  is non-empty, and is closed under multiplication and under taking inverses.

**Proposition 1.2.5:** Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then  $\varphi$  is an injective (or one-to-one) function if and only if  $\ker \varphi = \{1_G\}$ .

### 1.3. Rings

**Definition 1.3.1:** A **ring** is an additive abelian group  $R$  together with a binary operation of multiplication

$$\cdot : R \times R \rightarrow R$$

which satisfies the following:

- multiplication is associative:  $\forall a, b, c \in R, (ab)c = a(bc)$ .
- there is a multiplicative identity:  $\exists 1 \in R, \forall a \in R, 1a = a1 = a$ .
- distribution laws:  $\forall a, b, c \in R, a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$ .

The ring  $R$  is **commutative** provided that  $\forall a, b \in R, ab = ba$ .

*Example 1.3.2:*

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are commutative rings.
- For a natural number  $n > 1$ , the ring  $\text{Mat}_n(\mathbb{Z})$  of  $n \times n$  matrices with coefficients in  $\mathbb{Z}$  is a non-commutative ring.

**Definition 1.3.3:** For a commutative ring  $R$ , an element  $a \in R$  is a **unit** provided that  $\exists v \in R, uv = vu = 1$ .

The set  $R^\times$  of units in  $R$  is a group under the multiplication of  $R$ .

### 1.4. Fields

**Definition 1.4.1:** A **field** is a commutative ring  $F$  such that  $\forall a \in F, a \neq 0 \Rightarrow a$  is a unit.

*Example 1.4.2:*  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  are fields, but  $\mathbb{Z}$  is not a field.

### 1.5. Linear Algebra

**Definition 1.5.1:** If  $F$  is a field, a vector space over  $F$  – or an  $F$ -vector space – is an additive abelian group  $V$  together with an operation of scalar multiplication

$$F \times V \rightarrow V$$

written  $(t, v) \mapsto tv$ , subject to the following:

- identity:  $\forall v \in V, 1v = v$ .
- associativity:  $\forall a, b \in F$  and  $v \in V, a(bv) = (ab)v$ .
- distributive laws:  $\forall a, b \in F$  and  $v, w \in V, (a + b)v = av + bv$  and  $a(v + w) = av + aw$ .

*Remark 1.5.2:* Probably in a linear algebra class you saw results stated for vector spaces over  $\mathbb{R}$  or  $\mathbb{C}$ ; however, “most” results in linear algebra remain valid for vector space over  $F$ .

*Example 1.5.3:* Let  $I$  be any set, and let  $V$  be the set of all functions  $f : I \rightarrow F$  which have finite support. Recall that the support of  $f$  is  $\{x \in I \mid f(x) \neq 0\}$ .

Then  $V$  is a vector space. (The addition and scalar multiplication operations are define “pointwise” – see homework.)

*Remark 1.5.4:* Recall that a **basis** of a vector space is subset  $B$  of  $V$  which is linearly indepent and spans  $V$ .

The vector space of finitely supported functions  $I \rightarrow F$  has a basis  $B = \{\delta_i \mid i \in I\}$ , where

$$\delta_i : I \rightarrow F$$

is the function defined by  $\delta_i(j) = 0$  if  $i \neq j$  and  $\delta_i(i) = 1$ .

**Definition 1.5.5:** If  $V$  and  $W$  are  $F$ -vector spaces, an  $F$ -linear map  $\varphi : V \rightarrow W$  is a homomorphism of additive groups which satisfies the condition

$$\forall t \in F, \forall v \in V, \varphi(tv) = t\varphi(v).$$

**Definition 1.5.6:** If  $V$  is an  $F$ -vector space, the general linear group  $\text{GL}(V)$  is the set

$$\{\varphi : V \rightarrow V \mid \varphi \text{ is } F\text{-linear and invertible.}\}$$

$\text{GL}(V)$  is a group whose operation is given by composition of linear transformations.

*Remark 1.5.7:* If  $V$  is finite dimensional, so that  $V$  is isomorphic to  $F^n$  as  $F$ -vector spaces, linear algebra shows that  $\text{GL}(V)$  is isomorphic to the group  $\text{GL}_n$  of  $n \times n$  matrices with non-zero determinant, where  $n = \dim_F V$  and where the operation in  $\text{GL}_n$  is given by matrix multiplication.

## 1.6. Cayley’s Theorem

Let  $\Omega$  be any set. The set  $S(\Omega)$  of all bijective functions  $\psi : \Omega \rightarrow \Omega$  is a group whose operation is composition of functions.

**Theorem 1.6.1** (Cayley’s Theorem): Let  $G$  be any group. Then  $G$  is isomorphic to a subgroup of  $S(\Omega)$  for some  $\Omega$ .

*Proof:* Let  $\Omega = G$ . For  $g \in G$ , define a mapping  $\lambda_g : G \rightarrow G$  by the rule

$$\lambda_g(h) = gh.$$

We are going to argue that the mapping  $g \mapsto \lambda_g$  defines an injective group homomorphism  $G \rightarrow S(\Omega) = S(G)$ .

First of all, we note that  $\lambda_1 = \text{id}$ . Indeed, to check this identity of functions, let  $h \in \Omega = G$ . Then

$$\lambda_1(h) = 1h = h = \text{id}(h);$$

this confirms  $\lambda_1 = \text{id}$ .

Next, we note that for  $g_1, g_2 \in G$ , we have  $(*) \quad \lambda_{g_1} \circ \lambda_{g_2} = \lambda_{g_1 g_2}$ . Again, to confirm this identify of functions, we let  $h \in \Omega = G$ . Then

$$(\lambda_{g_1} \circ \lambda_{g_2})h = \lambda_{g_1}(\lambda_{g_2}(h)) = \lambda_{g_1}(g_2h) = g_1(g_2h) = (g_1g_2)h = \lambda_{g_1g_2}(h)$$

as required.

Now, using (\*) we see for  $g \in G$  that  $\lambda_g \circ \lambda_{g^{-1}} = \lambda_1 = \text{id} = \lambda_{g^{-1}} \circ \lambda_g$ , which proves that  $\lambda_g$  is bijective; thus indeed  $\lambda_g \in S(\Omega) = S(G)$ .

Moreover, (\*) shows that the mapping  $\lambda : G \rightarrow S(G)$  given by  $g \mapsto \lambda_g$  is a group homomorphism.

It remains to see that  $\lambda$  is injective. If  $g \in \ker \lambda$ , then  $\lambda_g = \text{id}$ . Thus  $1 = \text{id}(1) = \lambda_g(1) = g1 = g$ . Thus  $g = 1$  so that  $\ker \lambda = \{1\}$  which confirms that  $\lambda$  is injective by [Proposition 1.2.5](#). This completes the proof. ■

## 1.7. A linear analogue of Cayley's Theorem.

Let  $F$  be a field.

**Theorem 1.7.1:** Let  $G$  be any group. Then  $G$  is isomorphic to a subgroup of  $\text{GL}(V)$  for some  $F$ -vector space  $V$ .

*Proof:* The proof is quite similar to the proof of Cayley's Theorem.

Let  $V$  be the vector space of all finitely supported functions  $f : G \rightarrow F$ . Recall that  $V$  has a basis  $B = \{\delta_g \mid g \in G\}$ .

We are going to define an injective group homomorphism  $G \rightarrow \text{GL}(V)$ .

For  $g \in G$ , we may define an  $F$ -linear mapping  $\lambda_g : V \rightarrow V$  by defining the value of  $\lambda_g$  at each vector in  $B$ . We set  $\lambda_g(\delta_h) = \delta_{gh}$ .

Recall that a typical element  $v$  of  $V$  has the form

$$v = \sum_{i=1}^n t_i \delta_{h_i}$$

for scalars  $t_i \in F$  and elements  $g_i \in G$ ; since  $\lambda_g$  is  $F$ -linear, we have

$$\lambda_g(v) = \sum_{i=1}^n t_i \delta_{gh_i}.$$

We now show that  $\lambda_1 = \text{id}$ . To prove this, since the functions  $V \rightarrow V$  are linear, it is enough to argue that the functions agree at each element of the basis  $B$  of  $V$ . Well, for  $h \in G$ ,

$$\lambda_1(\delta_h) = \delta_{1h} = \delta_h = \text{id}(\delta_h)$$

as required.

We next show for  $g_1, g_2 \in G$  that (\*)  $\lambda_{g_1} \circ \lambda_{g_2} = \lambda_{g_1g_2}$ . Again, it suffices to argue that these functions agree at each element  $\delta_h$  of  $B$ . For  $h \in G$  we have:

$$(\lambda_{g_1} \circ \lambda_{g_2})(\delta_h) = \lambda_{g_1}(\lambda_{g_2}\delta_h) = \lambda_{g_1}(\delta_{g_2h}) = \delta_{g_1(g_2h)} = \delta_{(g_1g_2)h} = \lambda_{g_1g_2}\delta_h$$

as required.

Now, for  $g \in G$  we see that by (\*) that

$$\text{id} = \lambda_1 = \lambda_g \circ \lambda_{g^{-1}}$$

which proves that  $\lambda_g$  is invertible and hence in  $\text{GL}(V)$ .

Moreover, (\*) shows that the assignment  $\lambda : G \rightarrow \text{GL}(V)$  given by the rule  $g \mapsto \lambda_g$  is a group homomorphism.

It remains to argue that  $\lambda$  is injective. Suppose that  $x \in \ker \lambda$ , so that  $\text{id} = \lambda_x$ .

Then  $\delta_1 = \text{id}(\delta_1) = \lambda_x(\delta_1) = \delta_{x1} = \delta_x$ . This implies that  $1 = x$  so that indeed the kernel of  $\lambda$  is trivial and thus  $\lambda$  is injective by [Proposition 1.2.5](#).

■

## 2. Week 2 [2025-09-08]

This week, we'll discuss **quotients**, and we'll begin our discussion of **group actions**.

### 2.1. The Quotient of a set by an equivalence relation

Let  $S$  be a set and let  $R$  be a relation on  $S$ . Formally,  $R$  is an assignment  $R : S \times S \rightarrow \text{Prop}$  – in other words, for  $a, b \in S$ ,  $R(a, b)$  is the **proposition** that  $a$  and  $b$  are related; of course  $R(a, b)$  may or may not hold.

We often use a symbol  $\sim$  or  $\sim_R$  to indicate this proposition; thus  $R(a, b) \Leftrightarrow a \sim_R b$ .

**Definition 2.1.1:** The relation  $\sim$  is an **equivalence relation** if the following properties hold:

- **reflexive:**  $\forall s \in S, s \sim s$ .
- **symmetric:**  $\forall s_1, s_2 \in S, s_1 \sim s_2 \Rightarrow s_2 \sim s_1$
- **transitive:**  $\forall s_1, s_2, s_3 \in S, s_1 \sim s_2 \text{ and } s_2 \sim s_3 \Rightarrow s_1 \sim s_3$

**Definition 2.1.2:** If  $\sim$  is an equivalence relation on the set  $S$ , a **quotient** of  $S$  by  $\sim$  is a set  $\bar{S}$  together with a surjective function  $\pi : S \rightarrow \bar{S}$  with the following properties:

(Quot 1)  $\forall a, b \in S, a \sim b \Rightarrow \pi(a) = \pi(b)$

(Quot 2) Let  $T$  be any set and let  $f$  be any function  $f : S \rightarrow T$  such that  $\forall a, b \in S, a \sim b \Rightarrow f(a) = f(b)$ . Then there is a function  $\bar{f} : \bar{S} \rightarrow T$  for which  $f = \bar{f} \circ \pi$ .

**Proposition 2.1.3:** Suppose that  $(\bar{S}_1, \pi_1)$  and  $(\bar{S}_2, \pi_2)$  are two quotients of the set  $S$  by the equivalence relation  $\sim$ . Let

$$\bar{\pi}_2 : \bar{S}_1 \rightarrow \bar{S}_2$$

be the mapping determined by the quotient property for  $(\bar{S}_1, \pi_1)$  using

$$T = \bar{S}_2 \text{ and } f = \pi_2 : S \rightarrow \bar{S}_2,$$

and let

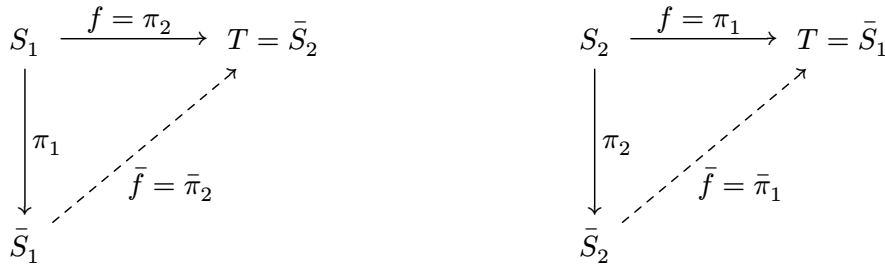
$$\bar{\pi}_1 : \bar{S}_2 \rightarrow \bar{S}_1$$

be the mapping determined by the quotient property for  $(\bar{S}_2, \pi_2)$  using

$$T = \bar{S}_1 \text{ and } f = \pi_1 : S \rightarrow \bar{S}_1.$$

Then the maps  $\pi'_2 : \bar{S}_1 \rightarrow \bar{S}_2$  and  $\pi'_1 : \bar{S}_2 \rightarrow \bar{S}_1$  are inverse to one another, and in particular  $\pi'_1$  and  $\pi'_2$  are bijections.

*Proof:* By the definition of quotients, we have commutative diagrams



In particular, we have  $\pi_2 = \bar{\pi}_2 \circ \pi_1$  and  $\pi_1 = \bar{\pi}_1 \circ \pi_2$

Substitution now yields

$$\pi_1 = \bar{\pi}_1 \circ \bar{\pi}_2 \circ \pi_1$$

and

$$\pi_2 = \bar{\pi}_2 \circ \bar{\pi}_1 \circ \pi_2$$

Since  $\pi_1$  and  $\pi_2$  are surjective, we conclude that  $\text{id} = \bar{\pi}_1 \circ \bar{\pi}_2$  and  $\text{id} = \bar{\pi}_2 \circ \bar{\pi}_1$  so indeed the indicated functions are inverse to one another. ■

*Remark 2.1.4:* The point of the Proposition is that a quotient is completely determined by the property indicated in the definition – this property is an example of what is known as a **universal property** or sometimes as a **universal mapping property**. The conclusion of the Proposition shows that any two ways of constructing a quotient are equivalent in a strong sense.

One way of constructing the quotient is by considering equivalence classes, as follows:

**Definition 2.1.5:** For an equivalence relation  $\sim$  on a set  $S$ , the **equivalence class**  $[s]$  of an element  $s \in S$  is the subset of  $S$  defined by

$$[s] = \{x \in S \mid x \sim s\}.$$

**Proposition 2.1.6:** Equivalence classes for the equivalence relation  $\sim$  have the following properties for arbitrary  $s, s' \in S$ :

- a.  $s \sim s' \Leftrightarrow [s] = [s']$
- b.  $[s] \neq [s'] \Leftrightarrow [s] \cap [s'] = \emptyset$

*Proof:* Review! ■

**Theorem 2.1.7 (Existence of quotients):** For any equivalence relation  $\sim$  on a set  $S$ , there is a quotient  $(\bar{S}, \pi)$ .

*Proof:* We consider the set  $\bar{S} = \{[s] \mid s \in S\}$  of equivalence classes and the mapping  $\pi : S \rightarrow \bar{S}$  given by the rule  $\pi(s) = [s]$ .



[Proposition 2.1.6](#) confirms condition (a) of [Definition 2.1.2](#).

For condition (b) of [Definition 2.1.2](#) suppose that  $T$  is a set and that  $f : S \rightarrow T$  is a function with the property that  $\forall a, b \in S, a \sim b \Rightarrow f(a) = f(b)$ . We must exhibit a function  $\bar{f} : \bar{S} \rightarrow T$  with the property  $f = \bar{f} \circ \pi$ . If  $\bar{f}$  exists, it must satisfy  $\bar{f}([a]) = f(a)$  for  $a \in S$ . On the other hand, in view of [Proposition 2.1.6](#) (a), the rule  $[a] \mapsto f(a)$  indeed determines a well-defined function  $\bar{f} : \bar{S} \rightarrow T$ . Moreover, the identity  $f = \bar{f} \circ \pi$  evidently holds. ■

*Remark 2.1.8:* We gave an explicit construction of the quotient using equivalence classes. On the other hand, if one has a quotient  $(\bar{S}, \pi)$ , the equivalence class  $[x]$  of an element  $x \in S$  is equal to  $\pi^{-1}(\pi(x))$ .

**Proposition 2.1.9:** If  $\sim$  is an equivalence relation on the set  $S$ , then  $S$  is the disjoint union of the equivalence classes.

*Proof:* Each element  $x \in S$  is contained in the equivalence classes  $[x]$ , so it only remains to prove that if two equivalence classes have a common element, they are equal. For this, let  $x, y \in S$  and suppose that  $z \in [x] \cap [y]$ . Then  $x \sim z$  and  $y \sim z$  so that  $x \sim y$  by transitivity; thus  $[x] = [y]$ . ■

## 2.2. Sub-groups

Let  $G$  be a group (when giving definitions, we'll write  $G$  multiplicatively).

**Definition 2.2.1:** A **subgroup** of  $G$  is a non-empty subset  $H \subseteq G$  such that  $H$  is closed under the operations of multiplication in  $G$  and inversion in  $G$ . In other words,

$$\forall a, b \in G, ab \in H \text{ and } a^{-1} \in H$$

*Example 2.2.2:* Consider the group  $G = \mathbb{Z} \times \mathbb{Z}$  where the operation is componentwise addition. Check the following!

- $H_1 = \{(a, b) \in G \mid 2a + 3b = 0\}$  is a subgroup.
- $H_2 = \{n(2, 2) + m(1, 2) \mid n, m \in \mathbb{Z}\}$  is a subgroup.

The collection of subgroups of  $G$  has a natural partial order given by *containment*.

**Proposition 2.2.3:** (Constructing subgroups)

- If  $H_i$  for  $i \in I$  is a family of subgroups of  $G$ , indexed by some set  $I$ , then the intersection  $\bigcap_{i \in I} H_i$  is again a subgroup of  $G$ .
- Let  $S \subseteq G$  be a subset. There is a unique smallest subgroup  $H(S) = \langle S \rangle$  containing  $S$ . In other words, for any subgroup  $H'$  of  $G$  with  $S \subseteq H'$ , we have  $\langle S \rangle \subseteq H'$ .

*Remark 2.2.4:*

- If  $S, T \subseteq G$  are subsets, we often write  $\langle S, T \rangle$  for  $\langle S \cup T \rangle$ . If  $S = \{s_1, s_2, \dots, s_n\}$  we often write  $\langle S \rangle = \langle s_1, s_2, \dots, s_n \rangle$ .
- The subgroup in [Example 2.2.2\(b\)](#) is precisely  $\langle (2, 2), (1, 2) \rangle$ .

- c. For any group  $G$  and  $a \in G$ ,  $\langle a \rangle := \langle \{a\} \rangle$  is the **cyclic subgroup** generated by  $a$ . If  $G$  is multiplicative, then  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$  while if  $G$  is additive then  $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$ .

**Proposition 2.2.5:** If  $\varphi : G \rightarrow H$  is a group homomorphism, then  $\ker \varphi$  is a subgroup of  $G$ .

**Proposition 2.2.6:** If  $X \subseteq G$  is a non-empty subset of  $G$ , then  $X$  is a subgroup if and only if  
(\*)  $\forall a, b \in X, ab^{-1} \in X$ .

*Proof:* ( $\Rightarrow$ ): Immediate from the definition of a subgroup.

( $\Leftarrow$ ): Assume that (\*) holds. We must show that  $X$  is a subgroup.

We first argue that  $X$  contains the identity element. Since  $X$  is non-empty, there is an element  $x \in X$ . Condition (\*) then shows that  $xx^{-1} = 1 \in X$  as required.

We now show that  $X$  is closed under inversion. Let  $x \in X$ . Since  $1 \in X$ , we apply (\*) with  $a = 1$  and  $b = x$  to learn that  $1x^{-1} = x^{-1} \in X$ , as required.

Finally, we show that  $X$  is closed under multiplication. Let  $x, y \in X$ . We have already seen that  $y^{-1} \in X$ . Now apply (\*) with  $a = x$  and  $b = y^{-1}$  to learn that

$$ab^{-1} = x(y^{-1})^{-1} = xy \in X$$

as required. ■

**Proposition 2.2.7:** Let  $f : G \rightarrow H$  be a group homomorphism and let  $S \subseteq G$  be any subset. Then

$$f(\langle S \rangle) \subseteq \langle f(S) \rangle.$$

*Proof:* Since  $f$  is a homomorphism, for any subgroup  $K \subseteq G$ , the image

$$f(K) = \{f(x) \mid x \in K\}$$

is a subgroup of  $H$ . Thus  $f(\langle S \rangle)$  is a subgroup containing  $\langle f(S) \rangle$  of  $H$  where  $f(S)$  is the image of the set  $S$  via the function  $f$ . It now follows from [Proposition 2.2.3](#) that  $f(\langle S \rangle)$  is contained in the subgroup  $\langle f(S) \rangle$  generated by  $f(S)$ , as required. ■

## 2.3. Group actions

**Definition 2.3.1:** Let  $G$  be a group and let  $\Omega$  be a set. An **action** of  $G$  on  $\Omega$  is a mapping

$$G \times \Omega \rightarrow \Omega \text{ written } (g, x) \mapsto gx$$

such that for each  $x \in \Omega$  we have

- $1x = x$
- $\forall g, h \in G, (gh)x = g(hx)$ .

For brevity, sometimes we say that  $\Omega$  is a  $G$ -space.

**Proposition 2.3.2:** An action of a group  $G$  on a set  $\Omega$  determines a homomorphism  $f : G \rightarrow S(\Omega)$  such that  $f(g)(x) = gx$  for  $g \in G$  and  $x \in \Omega$ .

Conversely, given a homomorphism  $f : G \rightarrow S(\Omega)$ , there is an action of  $G$  on  $\Omega$  given by  $gx = f(g)(x)$  for each  $g \in G$  and  $x \in \Omega$ .

**Definition 2.3.3:** Suppose that  $\Omega$  is a  $G$ -space. The  $G$ -conjugacy relation on  $\Omega$  is defined as follows: for  $x, y \in \Omega$ ,  $x \sim_G y$  provided that  $\exists g \in G, gx = y$ .

**Proposition 2.3.4:** The  $G$ -conjugacy relation on  $\Omega$  is an equivalence relation.

**Definition 2.3.5:** Let  $\Omega$  be a  $G$ -space, and let  $\varphi : \Omega \rightarrow \Omega / \sim$  be the quotient mapping for the  $G$ -conjugacy relation; see [Definition 2.1.2](#). For  $x \in \Omega$ , the **orbit**  $\mathcal{O}_x = Gx$  of  $G$  through  $x$  is the subset of  $\Omega$  defined by

$$\mathcal{O}_x = \varphi^{-1}(\varphi(x)).$$

Thus the  $G$ -orbits are the equivalence classes for the relation  $\sim_G$ ; see [Remark 2.1.8](#).

Equivalently, we have  $\mathcal{O}_x = \{gx \mid g \in G.\}$

**Proposition 2.3.6:**  $\Omega$  is the disjoint union of the  $G$ -orbits in  $\Omega$ .

*Proof:* This follows from [Proposition 2.1.9](#). ■

*Remark 2.3.7:* Each orbit  $\mathcal{O}_x$  is itself a  $G$ -set.

## 2.4. Quotients of groups

Let  $G$  be a group and let  $H$  be a subgroup of  $G$ . There is an action of  $H$  on the set  $G$  by right multiplication: for  $h \in H$  and  $g \in G$  we can define  $h \cdot g = gh^{-1}$ .

We are going to consider the quotient of  $G$  by the equivalence relation of  $H$ -conjugacy; this equivalence relation is defined by

$$g \sim g' \Leftrightarrow \exists h \in H, g = g'h.$$

**Definition 2.4.1:** The **left quotient of  $G$  by  $H$**  is the quotient  $(\pi, G/H)$  of  $G$  by the equivalence relation of  $H$ -conjugacy defined using the action of  $H$  on  $G$  by right multiplication as described above.

*Remark 2.4.2:*

- a. Of course, one can use an explicit model for the quotient by taking  $G/H$  to be the set of equivalence classes in  $G$  for the  $H$ -conjugacy relation.

- b. The equivalence classes for the relation of  $H$ -conjugacy defined by the action of right multiplication are precisely the **left cosets** of  $H$  in  $G$ . The class of  $x \in G$  has the form

$$xH = \{xh \mid h \in H\}$$

.

For  $x \in G$ ,

$$\pi^{-1}(\pi(x)) = xH.$$

- c. We can also consider the action of  $H$  on  $G$  by left multiplication. This action determines an equivalence relation of  $H$ -conjugacy, and the quotient of  $G$  by this equivalence relation is called the **right quotient of  $G$  by  $H$**  and is written  $(\pi, H \backslash G)$ . In this case, the equivalence classes are the **right cosets** where the class of  $x \in G$  has the form  $Hx = \{hx \mid h \in H\}$ .

For  $x \in G$ , we have  $\pi^{-1}(\pi(x)) = Hx$ .

**Proposition 2.4.3:** There is an action

$$\alpha : G \times G/H \rightarrow G/H$$

of the group  $G$  on the set  $G/H$  such that

$$\forall g, x \in G, \text{ we have } \alpha(g, \pi(x)) = \pi(gx)$$

where  $\pi : G \rightarrow G/H$  is the quotient map.

*Proof:* To define the action map  $\alpha$ , first fix  $g \in G$ . We are going to define the mapping

$$\alpha(g, -) : G/H \rightarrow G/H.$$

Consider the mapping  $\pi_g : G \rightarrow G/H$  given by the rule  $\pi_g(x) = \pi(gx)$ . This mapping has the property that  $x \sim_H x' \Rightarrow \pi_g(x) = \pi_g(x')$ . Indeed,

$$x \sim_H x' \Rightarrow \exists h, x = x'h \Rightarrow \pi_g(x) = \pi(gx) = \pi(gx'h) = \pi(gx') = \pi_g(x')$$

by the defining property of  $\pi$ ; see [Definition 2.1.2](#). Again using [Definition 2.1.2](#) we find the desired mapping  $\alpha(g, -) : G/H \rightarrow G/H$  with the property that

$$(\clubsuit) \quad \alpha(g, -) \circ \pi = \pi_g.$$

We now assemble the mappings  $\alpha(g, -)$  to get a mapping  $\alpha : G \times G/H \rightarrow G/H$  which satisfies  $\alpha(g, \pi(x)) = \pi(gx)$  for each  $g, x \in G$ , and it remains to check that  $\alpha$  determines an action as in [Definition 2.3.1](#).

Of course, using  $(\clubsuit)$ , we have  $\alpha(1, -) \circ \pi = \pi_1 = \pi = \text{id} \circ \pi$ ; since  $\pi$  is surjective, it follows that  $\alpha(1, -) = \text{id}$ . Thus  $\alpha(1, z) = z$  for each  $z \in G/H$ , which shows that  $\alpha$  satisfies the first requirement of [Definition 2.3.1](#).

Now suppose that  $g_1, g_2 \in G$ . To complete the proof, we must verify the remaining requirement of [Definition 2.3.1](#); thus we must show that

$$(\heartsuit) \quad \alpha(g_1, \alpha(g_2, -)) = \alpha(g_1 g_2, -)$$

On the one hand, using ( $\clubsuit$ ) we find that

$$\alpha(g_1 g_2, -) \circ \pi = \pi_{g_1 g_2};$$

on the other hand, for  $z \in G$  we have

$$\begin{aligned} (\alpha(g_1, \alpha(g_2, -)) \circ \pi)(z) &= \alpha(g_1, \alpha(g_2, \pi(z))) \\ &= \alpha(g_1, \pi_{g_2}(z)) \quad \text{by } (\clubsuit) \\ &= \alpha(g_1, \pi(g_2 z)) \\ &= \pi(g_1(g_2 z)) \quad \text{by } (\clubsuit) \end{aligned}$$

Since  $\pi$  is surjective, ( $\heartsuit$ ) follows at once. This completes the proof. ■

## 2.5. Quotients of groups and orbits.

**Definition 2.5.1:** Suppose that  $G$  acts on  $\Omega_1$  and on  $\Omega_2$ . A morphism of  $G$ -sets  $\varphi : \Omega_1 \rightarrow \Omega_2$  is a function  $\varphi$  with the property that  $\forall g \in G$  and  $\forall x \in \Omega_1$ , we have  $\varphi(gx) = g\varphi(x)$ .

The morphism of  $G$ -sets  $\varphi$  is an isomorphism (of  $G$ -sets) if there is a morphism of  $G$ -sets  $\psi : \Omega_2 \rightarrow \Omega_1$  such that  $\varphi \circ \psi = \text{id}$  and  $\psi \circ \varphi = \text{id}$ .

Suppose that  $G$  acts on  $\Omega$  and let  $x \in \Omega$ .

**Definition 2.5.2:** The **stabilizer of  $x$  in  $G$**  is the subgroup  $\text{Stab}_G(x) = \{g \in G \mid gx = x\}$ .

**Proposition 2.5.3:** Write  $H = \text{Stab}_G(x)$  and recall that  $\pi : G \rightarrow G/H$  is the quotient mapping. There is a unique isomorphism of  $G$ -sets  $\gamma : G/H \rightarrow \mathcal{O}_x$  with the property that

$$\gamma(\pi(1)) = x.$$

*Proof:* The rule  $g \mapsto gx$  determines a surjective mapping  $\alpha_x : G \rightarrow \mathcal{O}_x$ . Recall that the action of  $H$  on  $G$  by right multiplication determines an equivalence relation  $\sim$  on  $G$  used to construct the quotient  $G/H$ .

For  $g_1, g_2 \in G$  we find that

$$g_1 \sim g_2 \Rightarrow \exists h \in H, g_1 = g_2 h \Rightarrow \alpha_x(g_1) = \alpha_x(g_2 h) = g_2 h x = g_2 x = \alpha_x(g_2)$$

since  $h \in H = \text{Stab}_G(x) \Rightarrow hx = x$ .

Thus [Definition 2.1.2](#) shows that there is a mapping  $\gamma : G/H \rightarrow \mathcal{O}_x$  such that  $\gamma \circ \pi = \alpha_x$ . To see that  $\gamma$  is a morphism of  $G$ -sets, it suffices to show that ( $\clubsuit$ )  $\forall g, g'$  we have

$$\gamma(g \cdot \pi(g')) = g \cdot \gamma(\pi(g')).$$

Now by the definition of the  $G$ -action on  $G/H$  we have  $g \cdot \pi(g') = \pi(gg')$ ; see [Proposition 2.4.3](#). Thus  $\gamma(g \cdot \pi(g')) = \gamma(\pi(gg')) = \alpha_x(gg') = gg' \cdot x$ . On the other hand,  $g \cdot \gamma(\pi(g')) = g \cdot \alpha_{x(g')} = g \cdot g' \cdot x$  which confirms ( $\clubsuit$ ). This shows that  $\gamma$  is indeed a morphism of  $G$ -sets.

Since  $\alpha_x$  is surjective and  $\gamma \circ \pi = \alpha_x$ , also  $\gamma$  is surjective. It only remains to see that  $\gamma$  is injective. Suppose that  $z, z' \in G/H$  such that  $\gamma(z) = \gamma(z')$ . Since  $\pi : G \rightarrow G/H$  is surjective, we may choose  $g, g' \in G$  with  $z = \pi(g)$  and  $z' = \pi(g')$ . Now

$$\gamma(z) = \gamma(z') \Rightarrow \gamma(\pi(g)) = \gamma(\pi(g')) \Rightarrow \alpha_{x(g)} = \alpha_{x(g')} \Rightarrow gx = g'x.$$

We now conclude that  $g^{-1}gx = x$  so that  $g^{-1}g \in \text{Stab}_G(x) = H$ . Since the quotient mapping  $\pi$  is constant on  $H$ -orbits,  $z = \pi(g) = \pi(gg^{-1}g') = \pi(g') = z'$ . This shows that  $\gamma$  is injective and completes the proof. ■

**Definition 2.5.4:** The action of  $G$  on  $\Omega$  is **transitive** if there is a single  $G$ -orbit on  $\Omega$ . Equivalently, the action is transitive if the quotient  $\Omega / \sim$  is a singleton set.

*Example 2.5.5:* Let  $I$  be a set and let  $G = S(I)$  be the group of permutations of  $I$ . Fix  $x \in I$  and let  $H = \text{Stab}_G(x)$ . Notice that  $G$  acts on  $I$ . Moreover, the  $G$ -orbit of  $x$  is precisely  $I$  - in other words, the action of  $G$  on  $I$  is transitive.

Notice that  $H = S(I - \{x\})$ .

Now [Proposition 2.5.3](#) gives an isomorphism of  $G$ -sets  $G/H \rightarrow I$ ; i.e.  $S(I)/S(I - \{x\}) \rightarrow I$ .

## 2.6. The product of subgroups

**Definition 2.6.1:** If  $H, K \subseteq G$  are two subgroups, then  $H$  **normalizes**  $K$  if for each  $g \in H$  we have  $\text{Inn}_g K \subseteq K$  (in other words,  $\forall x \in K, gxg^{-1} \in K$ ).

**Definition 2.6.2:** Let  $H, K$  be subsets of  $G$ . The product of  $H$  and  $K$  is the subset

$$HK := \{xy \mid x \in H, y \in K\}$$

**Proposition 2.6.3:** Suppose that  $H, K$  are subgroups of  $G$  and that  $H$  normalizes  $K$ . Then  $\langle H, K \rangle = HK$ . In particular,  $HK$  a subgroup of  $G$ .

*Proof:* Let  $X = HK$ . Since any subgroup of  $G$  which contains both  $H$  and  $K$  clearly contains  $X$ , it only remains to argue that  $X$  is a subgroup. For this, we use [Proposition 2.2.6](#). First note that  $1 = 1 \cdot 1 \in X$ , so  $X$  is non-empty. Now, let  $a_1, b_2 \in X$ . We must argue that  $a_1 a_2^{-1} \in X$ . By definition, there are elements  $x_1, x_2 \in H$  and  $y_1, y_2 \in K$  with  $a_i = x_i y_i$  for  $i = 1, 2$ . We now compute

$$a_1 a_2^{-1} = x_1 y_1 (x_2 y_2)^{-1} = x_1 y_1 y_2^{-1} x_2^{-1} = (x_1 x_2^{-1}) \cdot (x_2 y_1 y_2^{-1} x_2^{-1}).$$

We notice that  $x_1x_2^{-1} \in H$ . Moreover,  $y_1y_2^{-1} \in K$ ; since  $H$  normalizes  $K$  it follows that  $x_2y_1y_2^{-1}x_2^{-1} \in K$ .

We have now argued that  $a_1a_2^{-1}$  has the form  $xy$  for  $x \in H$  and  $y \in K$  so that  $a_1a_2^{-1} \in X$ . Now [Proposition 2.2.6](#) indeed shows that  $X = HK$  is a subgroup. ■

**Proposition 2.6.4:** Let  $H, K$  be subgroups of  $G$  and let  $\varphi : H \times K \rightarrow HK$  be the natural mapping given by  $\varphi(h, k) = hk$ .

- For each  $\alpha \in HK$ , the set  $\varphi^{-1}(\alpha)$  is in bijection with  $H \cap K$ .
- In particular, if  $H \cap K = \{1\}$ , then  $\varphi$  is bijective.

*Proof:* Let  $\alpha = hk \in HK$ . Note for any  $x \in H \cap K$  that  $\varphi(hx, x^{-1}k) = \alpha$  so that  $(hx, x^{-1}k) \in \varphi^{-1}(\alpha)$ . We argue that the mapping

$$\gamma : H \cap K \rightarrow \varphi^{-1}(\alpha) \text{ given by } \gamma(x) = (hx, x^{-1}k)$$

is bijective. Well, if  $(h_1, k_1) \in \varphi^{-1}(\alpha)$  then  $\varphi(h_1, k_1) = \varphi(h, k)$  so that  $h_1k_1 = hk$  and thus  $h^{-1}h_1 = kk_1^{-1}$ . Now set  $x = h^{-1}h_1 = kk_1^{-1} \in H \cap K$  and observe that  $(h_1, k_1) = \gamma(x)$ . This shows that  $\gamma$  is surjective. To see that  $\gamma$  is injective, suppose that  $\gamma(x) = \gamma(x')$  for  $x \in H \cap K$ . Then

$$(hx, x^{-1}k) = (hx', x'^{-1}k) \Rightarrow hx = hx' \Rightarrow x = x'.$$

So  $\gamma$  is injective and the proof of a. is complete.

Now, the mapping  $\varphi$  is surjective by the definition of  $HK$ . To prove b. we suppose that

$$H \cap K = \{1\}.$$

According to a. the fiber  $\varphi^{-1}(\alpha)$  is a singleton for each  $\alpha \in HK$ ; this shows that  $\varphi$  is injective and confirms b. ■

**Corollary 2.6.5:** If  $G$  is a finite group and  $H, K$  subgroups of  $G$ , then

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

*Proof:* This is a consequence of [Proposition 2.6.4](#). ■

Let's introduce some examples of groups in order to investigate this a bit more.

*Example 2.6.6:* For  $n \in \mathbb{N}$  with  $n \geq 1$ , consider the symmetric group  $S = S_n$  viewed as  $S(\mathbb{Z}/n\mathbb{Z})$  where  $\mathbb{Z}/n\mathbb{Z}$  denotes the collection of integers modulo  $n$ .

Consider the elements  $\sigma, \tau \in S$  defined by the rules  $\sigma(i) = i + 1$  and  $\tau(i) = -i$  where the addition and negation occurs in  $\mathbb{Z}/n\mathbb{Z}$ .

Viewed as permutations,  $\sigma$  identifies with an  $n$ -cycle and  $\tau$  identifies with a product of disjoint transpositions:

$$\sigma = (1, 2, \dots, n) \text{ and } \tau = (1, n-1)(2, n-2)\dots = \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (i, n-i).$$

In particular,  $\sigma$  has order  $n$  and  $\tau$  has order 2. Moreover,

$$(\heartsuit) \quad \tau\sigma\tau = \sigma^{-1}$$

Condition  $(\heartsuit)$  shows that the subgroup  $\langle \tau \rangle$  normalizes the subgroup  $\langle \sigma \rangle$ . Thus [Proposition 2.6.3](#) shows that

$$\langle \sigma, \tau \rangle = \langle \sigma \rangle \langle \tau \rangle.$$

We call  $D = \langle \sigma, \tau \rangle$  the **dihedral group** of order  $n$ . Note that  $(\heartsuit)$  shows that  $\langle \tau \rangle$  normalizes  $\langle \sigma \rangle$  so that  $D = \langle \tau \rangle \cdot \langle \sigma \rangle$ .

We claim:

- $|D| = 2n$ . In fact,  $D$  is usually written  $D_{2n}$ .

To prove the claim, we apply [Corollary 2.6.5](#); we just need to argue that

$$(\clubsuit) \quad \langle \sigma \rangle \cap \langle \tau \rangle = \{1\}.$$

Since  $\sigma$  has order  $n$  and  $\tau$  has order 2,  $(\clubsuit)$  is immediate if  $n$  is odd.

Now suppose that  $n = 2k$  is even. The unique subgroup of order 2 in  $\langle \sigma \rangle$  is generated by  $\sigma^k$ . To prove  $(\clubsuit)$  we must argue that  $\sigma^k \neq \tau$ .

Suppose the contrary. If  $\sigma^k = \tau$  then  $\sigma(n) = \tau(n) \in \mathbb{Z}/n\mathbb{Z}$ . Since  $\sigma^k(n) \equiv n + k \pmod{n}$  while  $\tau(n) = -n \equiv n \pmod{n}$ , we conclude that  $n + k \equiv n \pmod{n}$ ; thus  $k \equiv 0 \pmod{n}$  i.e.  $2k \mid k$ , which yields a contradiction as  $k \geq 1$ . This completes the proof  $(\clubsuit)$ .

## 2.7. Lagrange's Theorem

Let  $H$  be a subgroup of the group  $G$  and write  $G/H$  for the (left) quotient, as above. Recall that the  $H$ -cosets  $xH$  are the  $H$ -orbits for this action.

**Theorem 2.7.1:** There is a bijection  $\varphi : (G/H) \times H \rightarrow G$  for which  $\{\varphi(z, h) \mid h \in H\}$  is an  $H$ -orbit (i.e. a left  $H$ -coset) for each  $z \in G/H$ .

*Proof:* Indeed, using the axiom of choice we select for each  $z \in G/H$  an element  $g_z \in \pi^{-1}(z)$  where  $\pi : G \rightarrow G/H$  is the quotient map.

Now define  $\varphi : (G/H) \times H \rightarrow G$  by the rule  $\varphi(z, h) = g_z h$ .

To see that  $\varphi$  is onto, let  $g \in G$ . One then knows that  $g \sim g_z$  for some  $z \in G/H$ . Since  $\pi^{-1}(z) = g_z H$  it follows that  $g = g_z h$  for some  $h \in H$ , so  $g = \varphi(z, h)$ .

To see that  $\varphi$  is injective, suppose that  $\varphi(z, h) = \varphi(z', h')$ . Then  $g_z h = g_{z'} h'$  so that

$$(g_{z'})^{-1} g_z \in H \Rightarrow g_z \sim g_{z'} \Rightarrow z = z'.$$



Now  $g_z h = g_z h' \Rightarrow h = h'$  which completes the proof that  $\varphi$  is injective. The remaining assertion follows from the definition of  $\varphi$ . ■

**Corollary 2.7.2:** Suppose that  $G$  is a finite group and that  $H$  is a subgroup of  $G$ . Then

$$|G| = |G/H| \cdot |H|.$$

*Proof:* Indeed, for finite sets  $X$  and  $Y$ , we have  $|X \times Y| = |X| |Y|$ . ■

### 3. Week 3 [2025-09-15]

#### 3.1. Normal subgroups

Subgroups of the form  $\ker \varphi$  have a property that ordinary subgroups might lack; in this section we describe this property.

**Proposition 3.1.1:** Let  $G$  be a group.

- a. For  $g \in G$ , the assignment  $x \mapsto gxg^{-1}$  determines a group isomorphism

$$\text{Inn}_x : G \rightarrow G$$

- b. The assignment  $x \mapsto \text{Inn}_x$  determines a group homomorphism  $G \rightarrow \text{Aut}(G)$  where  $\text{Aut}(G)$  is the group of *automorphisms* of  $G$ .

*Proof sketch:*

- First check that  $\text{Inn}_x$  is a group homomorphism.
- Then check that  $(\blacklozenge) \text{Inn}_x \circ \text{Inn}_y = \text{Inn}_{xy}$  for all  $x, y \in G$ .
- Next, check that  $\text{Inn}_1 = \text{id}$ . Using  $(\blacklozenge)$ , this shows that  $(\text{Inn}_x)^{-1} = \text{Inn}_{x^{-1}}$  so indeed  $\text{Inn}_x$  is an *automorphism* of  $G$ .
- Finally,  $(\blacklozenge)$  shows that  $\text{Inn}$  is a group homomorphism.

■

**Definition 3.1.2:** A subset  $N \subseteq G$  is a **normal subgroup** of  $G$  if  $N$  is a subgroup of  $G$  and if for any  $g \in G$  and for any  $x \in N$ , we have  $gxg^{-1} \in N$ .

Using earlier notation, a subgroup  $N$  is normal if  $\forall g \in G, \text{Inn}_g N \subseteq N$ .

*Remark 3.1.3:* If  $N$  is a normal subgroup then for every  $g \in G$  we have  $\text{Inn}_g N = N$ .

Indeed, our assumption means for every  $g$  that  $\text{Inn}_g N \subseteq N$ . Thus  $\text{Inn}_g^{-1} \circ \text{Inn}_g N \subseteq \text{Inn}_g^{-1} N$  so that  $N \subseteq \text{Inn}_g^{-1} N$ . Since this holds for every  $g$ , we find that  $\text{Inn}_g N \subseteq N \subseteq \text{Inn}_g N$  for every  $g$ ; this confirms the assertion.

**Proposition 3.1.4:** Let  $H$  be a subgroup of  $G$ .

- a. Suppose  $G = \langle S \rangle$  for some subset  $S \subseteq G$ . Then  $H$  is normal in  $G$  if and only if  $\text{Inn}_x H = H$  for each  $x \in S$ .
- b. If  $H = \langle T \rangle$  for some subset  $T \subseteq H$ , then  $H$  is normal in  $G$  if and only if  $\forall t \in T, \forall x \in G, \text{Inn}_x t \in H$ .

*Proof:*

- a.  $(\Rightarrow)$ : This follows from the definition of normal subgroup.

( $\Leftarrow$ ): Write  $N = \{g \in G \mid \text{Inn}_g H = H\}$  and **check** that  $N$  is a subgroup of  $G$ . It is clear that  $H \subseteq N$  and by construction  $H$  is a normal subgroup of  $N$ . Now our assumption shows that  $S \subseteq N$  so that  $G = \langle S \rangle \subseteq N \Rightarrow N = G$  and thus  $H$  is normal in  $G$ .

b. ( $\Rightarrow$ ): Again, this implication follows from the definition of normal subgroup.

( $\Leftarrow$ ): Fix  $x \in G$ ; we must argue that  $\text{Inn}_x H \subseteq H$ . We know that  $\text{Inn}_x$  is a group homomorphism; see [Proposition 3.1.1](#). It follows from [Proposition 2.2.7](#)

$$\text{Inn}_x(\langle T \rangle) \subseteq \langle \text{Inn}_x(T) \rangle$$

which indeed shows that  $\text{Inn}_x H \subseteq H$ . ■

**Proposition 3.1.5:** Let  $N = \ker \varphi$  where  $\varphi : G \rightarrow H$  is a group homomorphism. Then  $N$  is a normal subgroup of  $G$ .

*Proof:* We have already observed that  $N$  is a subgroup. Now let  $g \in G$  and  $x \in N$  so that  $\varphi(x) = 1$ . Now

$$\varphi(\text{Inn}_g(x)) = \varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = 1$$

so that  $\text{Inn}_g N \subseteq N$  as required. ■

*Example 3.1.6:* Consider the group  $\text{GL}_2(\mathbb{Q})$ . For  $x \in \mathbb{Q}$  write

$$\alpha(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Note for  $x, y \in \mathbb{Q}$  that  $\alpha(x+y) = \alpha(x)\alpha(y)$ ; thus  $\alpha : \mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Q})$  is an injective group homomorphism whose image

$$U_{\mathbb{Q}} = \{\alpha(x) \mid x \in \mathbb{Q}\} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{Q} \right\}$$

is a subgroup of  $\text{GL}_2(\mathbb{Q})$ .

Observe that  $U_{\mathbb{Z}} = \{\alpha(x) \mid x \in \mathbb{Z}\}$  is a subgroup of  $U_{\mathbb{Q}}$ .

For  $t \in \mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$ , write

$$h(t) = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}.$$

For  $t, s \in \mathbb{Q}^{\times}$ , we have  $h(ts) = h(t)h(s)$  so that  $h : \mathbb{Q}^{\times} \rightarrow \text{GL}_2(\mathbb{Q})$  is an injective group homomorphism whose image

$$H = \{h(t) \mid t \in \mathbb{Q}^{\times}\} = \left\{ \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{Q}^{\times} \right\}$$

is a subgroup of  $\text{GL}_2(\mathbb{Q})$ .

We observe for  $t \in \mathbb{Q}^{\times}$  and  $x \in \mathbb{Q}$  that

$$h(t)\alpha(x)h(t)^{-1} = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & tx \\ 0 & 1 \end{pmatrix} = \alpha(tx).$$

This shows that  $\forall h \in H, \text{Inn}_h U_{\mathbb{Q}} \subseteq U_{\mathbb{Q}}$  so that  $H$  normalizes  $U_{\mathbb{Q}}$ .

Let  $n \in \mathbb{Z}$  with  $n > 1$  and consider the subgroup  $C = C_n = \langle h(n) \rangle$  of  $H$ .

The generator  $h(n)$  satisfies  $\text{Inn}_{h(n)} U_{\mathbb{Z}} \subset U_{\mathbb{Z}}$  since for  $x \in \mathbb{Z}$

$$h(n)\alpha(x)h(n)^{-1} = \alpha(nx) \in U_{\mathbb{Z}}.$$

Note however that  $\text{Inn}_{h(n)} U_{\mathbb{Z}}$  is a proper subset of  $U_{\mathbb{Z}}$ ; indeed, identifying  $U_{\mathbb{Z}}$  with  $\mathbb{Z}$ , the image subgroup  $\text{Inn}_{h(n)} U_{\mathbb{Z}}$  identifies with  $n\mathbb{Z}$  and of course  $n\mathbb{Z}$  has index  $n$  in  $\mathbb{Z}$ .

The group  $U_{\mathbb{Z}}$  is not normalized by  $C = \langle h(n) \rangle$  e.g. since  $\text{Inn}_{h(n)}^{-1} U_{\mathbb{Z}} = \text{Inn}_{h(n^{-1})} U_{\mathbb{Z}} \not\subseteq U_{\mathbb{Z}}$ ; indeed

$$\text{Inn}_{h(n^{-1})} \alpha(1) = \alpha\left(\frac{1}{n}\right) = \begin{pmatrix} 1 & \frac{1}{n} \\ 0 & 1 \end{pmatrix} \notin U_{\mathbb{Z}}.$$

This example shows the following: there exists a group  $G$ , subgroups  $H, K$  of  $G$ , and a subset  $S \subseteq G$  for which  $H = \langle S \rangle$  such that  $\text{Inn}_x K \subseteq K$  for all  $x \in S$  even though  $H$  does not normalize  $K$ .

Of course, if we insist that  $\text{Inn}_x K = K$  for all  $x \in S$  then  $H$  will normalize  $K$ ; see [Proposition 3.1.4](#).

In the proof of [Proposition 3.1.4](#) we gave a definition of the normalizer of  $K$  in  $H$ , namely

$$N_H(K) = \{h \in H \mid \text{Inn}_h K = K\}.$$

This example shows why in that definition one needs to insist that  $\text{Inn}_h K = K$  for each  $h \in H$  rather than simple  $\text{Inn}_h K \subseteq K$ .

## 3.2. Quotient groups

**Theorem 3.2.1:** Let  $N$  be a subgroup of  $G$ , and write  $(\pi_{G/N}, G/N)$  for the quotient. If  $N$  is a normal subgroup, then  $G/N$  is a group for which

a. the multiplication  $\mu : G/N \times G/N \rightarrow G/N$  satisfies

$$\forall g, g' \in G, \pi(g)\pi(g') = \pi(gg')$$

b. the identity is given by  $1_{G/N} = \pi(1_G)$ ,

c. inversion satisfies  $\forall g \in G, \pi(g)^{-1} = \pi(g^{-1})$ .

Moreover, the quotient map  $\pi_{G/N} : G \rightarrow G/N$  is a group homomorphism.

*Proof:* We first confirm that there is a mapping  $\mu : G/N \times G/N \rightarrow G/N$  satisfying the condition in a.

We observe that  $G/N \times G/N$  may be viewed as the quotient of the product group  $G \times G$  by the subgroup  $N \times N$ ; i.e. as  $(G \times G)/(N \times N)$ .

Consider the function

$$\varphi : G \times G \rightarrow G/N$$

given by

$$\varphi(g, g') = \pi_{G/N}(gg').$$

We claim that  $\varphi$  is constant on the  $N \times N$  orbits in  $G \times G$ . Indeed, suppose that  $(g, g') = (g_1, g'_1)(h, h')$  for  $g, g', g_1, g'_1 \in G$  and  $h, h' \in N$ . Thus  $g = g_1h$  and  $g' = g'_1h'$ . Then

$$\varphi(g, g') = \pi_{G/N}(gg') = \pi_{G/N}(g_1h \cdot g'_1h') = \pi_{G/N}(g_1g'_1g_1^{-1}hg'_1h') = \pi_{G/N}(g_1g'_1) = \varphi(g_1, g'_1)$$

since  $N$  a normal subgroup  $\Rightarrow g_1^{-1}hg'_1 \in N \Rightarrow g_1^{-1}hg'_1h' \in N$ . Thus there is a mapping  $\mu : G/N \times G/N \rightarrow G/N$  which satisfies  $\mu \circ \pi_{G \times G/N \times N} = \varphi$  and  $\mu$  clearly satisfies a.

Next we confirm that there is an inversion mapping  $G/N \rightarrow G/N$  that satisfies b. For this, one just checks that the mapping  $G \rightarrow G/N$  given by  $g \mapsto \pi_{G/N}(g^{-1})$  is constant on  $N$ -orbits. Let  $g, g' \in G$  and  $h \in N$  and suppose that  $g = g'h$ . We must argue that

$$\pi_{G/N}(g^{-1}) = \pi_{G/N}(g'^{-1}).$$

We have

$$(g'h)^{-1} = h^{-1}g'^{-1} = g'^{-1}g'h^{-1}g'^{-1}$$

so indeed

$$\pi_{G/N}(g^{-1}) = \pi_{G/N}((g'h)^{-1}) = \pi_{G/N}(g'^{-1}g'h^{-1}g'^{-1}) = \pi_{G/N}(g'^{-1})$$

since  $g'h^{-1}g'^{-1} \in N$  by the normality of  $N$  in  $G$ .

It remains to confirm that the group axioms hold.

To confirm associativity in  $G/N$ , let  $z, z', z'' \in G/N$ . We must argue that  $(zz')z'' = z(z'z'')$ . Since  $\pi$  is surjective we can write  $z = \pi(g)$ ,  $z' = \pi(g')$  and  $z'' = \pi(g'')$  for  $g, g', g'' \in G$ . Now we see using a. twice that

$$(zz')z'' = (\pi(g)\pi(g'))\pi(g'') = \pi(gg')\pi(g'') = \pi((gg')g'').$$

A similar calculation shows that

$$z(z'z'') = \pi(g(g'g''))$$

and now the result follows by associativity in  $G$ .

Similar calculations confirm that the  $\pi_{G/N}(1)$  acts as an identity and that  $\pi_{G/N}(g^{-1})$  is the inverse of  $\pi_{G/N}(g)$ .

Finally, it follows from the definitions that  $\pi_{G/N}$  is a group homomorphism. ■

*Example 3.2.2:*

If  $G$  is an abelian group, then  $\text{Inn}_x$  is the trivial homomorphism for each  $x \in G$ , and in particular every subgroup of  $G$  is normal.

Let's consider an additive abelian group  $A$  and  $B$  any subgroup. Write  $\pi : A \rightarrow A/B$  for the quotient mapping.

For  $a \in A$ , we often view  $\pi(a)$  as the coset  $a + B = \{a + x \mid x \in B\}$ .

We see for  $a, a' \in A$  that  $\pi(a) = \pi(a') \Leftrightarrow a - a' \in B$ .

### 3.3. First isomorphism theorem

**Theorem 3.3.1:** Let  $\varphi : G \rightarrow H$  be a group homomorphism, and let  $K = \ker \varphi$ . Assume that  $\varphi$  is surjective. Then there is a unique isomorphism of groups  $\bar{\varphi} : G/K \rightarrow H$  such that  $\varphi = \bar{\varphi} \circ \pi$  where  $\pi : G \rightarrow G/K$  is the quotient homomorphism.

*Proof:* We first observe that – provided it exists –  $\bar{\varphi}$  is unique. Indeed, for any  $z \in G/K$  we may write  $z = \pi(g)$  for  $g \in G$  and then our assumption guarantees that

$$(*) \quad \bar{\varphi}(z) = \bar{\varphi}(\pi(g)) = \varphi(g).$$

So it just remains to argue that  $(*)$  determines a group isomorphism.

We first check that  $(*)$  determines a group homomorphism. Indeed, for  $z, z' \in G/K$  with  $z = \pi(g)$  and  $z' = \pi(g')$  for  $g, g' \in G$ , we have

$$\bar{\varphi}(zz') = \bar{\varphi}(\pi(g)\pi(g')) = \bar{\varphi}(\pi(gg')) = \varphi(gg') = \varphi(g)\varphi(g') = \bar{\varphi}(\pi(g))\bar{\varphi}(\pi(g')) = \overline{\varphi(z)\varphi(z')}.$$

Now we observe that since  $\varphi$  is surjective, and since  $\pi : G \rightarrow G/K$  is surjective, then  $\bar{\varphi}$  is surjective.

Finally, we check that  $\varphi$  is injective. For this, it suffices to show that  $\ker \varphi = \{1\}$ ; see [Proposition 1.2.5](#).

So, let  $z \in \ker \varphi \subseteq G/K$  and write  $z = \pi(g)$  for  $g \in G$ . We know that

$$1_H = \bar{\varphi}(z) = \bar{\varphi}(\pi(g)) = \varphi(g)$$

and we conclude that  $\varphi(g) = 1 \Rightarrow g \in \ker \varphi$ . Since  $g \in \ker \varphi$ , we know that  $\pi(g) = \pi(1)$ , in other words,  $z = \pi(g)$  is the identity element of the quotient group  $G/K$ . This proves that  $\ker \bar{\varphi}$  is trivial so that  $\bar{\varphi}$  is injective. ■

### 3.4. Groups acting on Groups

Let  $G$  and  $H$  be groups and suppose that  $G$  acts on the set  $H$ .

**Definition 3.4.1:** We say that  $G$  acts by automorphisms on  $H$  if for each  $g \in G$ , the mapping

$$h \mapsto g \cdot h : H \rightarrow H$$

is an automorphism of the group  $H$ .

*Remark 3.4.2:* To give an action of  $G$  on  $H$  by automorphisms is the same as to give a group homomorphism  $G \rightarrow \text{Aut}(H)$ .

**Proposition 3.4.3:** If  $G$  acts on  $H$  by automorphisms, the set of fixed points  $H^G = \{x \in H \mid g \cdot x = x \forall g \in G\}$  is a subgroup of  $H$ .

*Proof:*  $1 \in H^G$  since each each group automorphism  $\psi : H \rightarrow H$  satisfies  $\psi(1) = 1$ .

Let  $x, y \in H^G$ . We must argue that  $x^{-1}y \in H^G$ .

We first argue that  $x^{-1} \in H^G$ . For this, let  $g \in G$ . Since the action of  $g$  is an automorphism of  $H$  and since  $g \cdot x = x$ , we see that

$$1 = g \cdot 1 = g \cdot xx^{-1} = (g \cdot x)(g \cdot x^{-1}) = x(g \cdot x^{-1}).$$

This shows that  $g \cdot x^{-1} = x^{-1}$  so that  $x^{-1} \in H^G$ .

Now again let  $g \in G$ . We must argue that  $g \cdot x^{-1}y = x^{-1}y$ . Since  $g$  acts as an automorphism of  $H$  we see that

$$g \cdot x^{-1}y = (g \cdot x^{-1})(g \cdot y) = x^{-1}y$$

since  $x^{-1}, y \in H^G$ . ■

*Example 3.4.4:*  $G$  acts in itself by inner automorphisms. This action is determined by the group homomorphism  $\text{Inn} : G \rightarrow \text{Aut}(G)$ .

In this case, the subgroup  $G^G = G^{\text{Inn}(G)}$  of fixed points is precisely the center  $Z = Z(G)$ :

$$Z = \{x \in G \mid \text{Inn}_g x = x\} = \{x \in G \mid gx = xg \quad \forall g \in G\}$$

For  $x \in G$ , the stabilizer  $\text{Stab}_G(x)$  is known as the centralizer:

$$\text{Stab}_G(x) = C_G(x) = \{g \in G \mid \text{Inn}_g x = x\} = \{g \in G \mid gx = xg\}.$$

And the orbit of  $x$  is known as the conjugacy class of  $x$ :

$$\mathcal{O}_x = \text{Cl}(x) = \{\text{Inn}_g x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}.$$

[Proposition 2.5.3](#) gives a bijection

$$\text{Cl}(x) \simeq G/C_G(x).$$

**Proposition 3.4.5:** The center of a group  $G$  is a normal subgroup of  $G$ .

### 3.5. $p$ -groups

**Definition 3.5.1:** For a prime number  $p$ , a finite  $p$ -group is a finite group  $G$  whose order is a power of  $p$ .

Let  $G$  be a finite  $p$ -group and suppose that  $G$  acts on the finite set  $E$ , and write  $E^G$  for the set of elements of  $E$  fixed by the action of  $G$ ; thus  $E^G = \{x \in E \mid \forall g \in G, g \cdot x = x\}$ .

**Proposition 3.5.2:** With notation as above, we have  $|E| \equiv |E^G| \pmod{p}$ .

*Proof:* Indeed, the complement  $E \setminus E^G$  is the disjoint union of non-trivial orbits of  $G$ , each of which has order divisible by  $p$ . ■

**Proposition 3.5.3:** Suppose that  $G$  acts by automorphisms on a second  $p$ -group  $H$ . The fixed points  $H^G$  form a non-trivial subgroup.

*Proof:* First of all, the fixed points form a subgroup because the action of an element  $g \in G$  is a group automorphism of  $H$ . In more detail, since  $H^G$  is a non-empty subset of  $G$ , it is enough to argue that for every  $x, y \in H^G$ , we have  $x^{-1}y \in H^G$ .

We first argue that  $x^{-1} \in H^G$ . For  $g \in G$ , we have

$$1 = g \cdot 1 = g \cdot xx^{-1} = (g \cdot x)(g \cdot x^{-1}) = x(g \cdot x^{-1}).$$

Thus  $g \cdot x^{-1}$  is an inverse of  $x$  so indeed  $x^{-1} = g \cdot x^{-1}$ . We now show that  $x^{-1}y \in H^G$ . For this again let  $g \in G$  be arbitrary. We have

$$g \cdot x^{-1}y = (g \cdot x^{-1})(g \cdot y) = x^{-1}y$$

which shows that  $x^{-1}y \in H^G$ .

Now [Proposition 3.5.2](#) shows that  $p$  divides the order of the subgroup  $H^G$ , so  $H^G$  is indeed non-trivial. ■

**Theorem 3.5.4:** The center of a non-trivial  $p$ -group is non-trivial.

*Proof:* If  $G$  is a non-trivial  $p$ -group, consider the action of  $G$  on itself by conjugation. The subgroup of fixed points is precisely the center of  $G$ , and [Proposition 3.5.3](#) implies that this subgroup is non-trivial. ■

**Corollary 3.5.5:** Let  $G$  be a finite  $p$ -group with  $|G| = p^n$ . There is a series of subgroups

$$\{1\} = G_n \subset G_{n-1} \subset \dots \subset G_0 = G$$

such that  $G_i$  is normal in  $G$  for each  $0 \leq i < n$  and such that  $G_i/G_{i+1}$  is cyclic of order  $p$  for  $0 \leq i < n - 1$ .

*Proof sketch:* We proceed by induction on  $|G|$ . If  $|G| = 1$  so that  $G$  is the trivial group, the assertion is immediate.

Now suppose given a non-trivial  $p$ -group  $G$  and suppose that the result holds for all  $p$ -groups of order  $< |G|$ .

Let  $Z$  be the center of  $G$ . Then  $Z$  is non-trivial by [Theorem 3.5.4](#). Thus  $G/Z$  is  $p$  group with order  $< |G|$ .



By induction there is a sequence of subgroups

$$\{1\} = H_m \subset H_{m-1} \subset \dots \subset H_0 = G/Z.$$

such that  $H_i$  is normal in  $G/Z$  and  $H_i/H_{i+1}$  is cyclic of order  $p$  for each  $i < m$ .

Let  $G_i = \pi^{-1}(H_i) \subset G$ , where  $\pi : G \rightarrow G/Z$  is the quotient homomorphism.

One must check the following:

- $G_i$  is a normal subgroup of  $G$ ,
- $G_i/G_{i+1} \simeq H_i/H_{i+1}$  is cyclic of order  $p$  for each  $i$ .

Since  $G_m = \ker \pi = Z$  we have the sequence in  $G$ :

$$\{1\} \subset Z = G_m \subset G_{m-1} \subset \dots \subset G_1 \subset G_0 = G.$$

Thus to complete the proof of the Theorem, we must demonstrate that  $Z$  has a suitable sequence of subgroup.

Thus it remains to prove the Theorem in case  $G$  is an *abelian*  $p$ -group. This proof is addressed in the homework. ■

### 3.6. Sylow subgroups

Let  $G$  be a finite group of order  $n = p^m q$  with  $p$  a prime and with  $\gcd(p, q) = 1$ .

**Theorem 3.6.1** (Sylow's Theorem): There exists a subgroup of  $G$  having order  $p^m$ ; such a subgroup is known as a *Sylow subgroup*, or a *Sylow  $p$ -subgroup*. Moreover:

- a. Any two Sylow  $p$ -subgroups are conjugate by an element of  $G$ .
- b. Any  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup.
- c. If  $r$  denotes the number of  $p$ -Sylow subgroups, then  $r \equiv 1 \pmod{p}$  and  $r \mid q$ .

For the proof, we consider the set  $E$  of all subsets of  $G$  having order  $p^m$ . The action of  $G$  on itself by translation induces an action of  $G$  on  $E$ : for  $X \in E$ , evidently  $g \cdot X \in E$  where  $g \cdot X = \{g \cdot x \mid x \in X\}$ .

One knows that  $|E| = \binom{|G|}{p^m} = \binom{p^m q}{p^m}$ .

**Proposition 3.6.2:**  $\binom{p^m q}{p^m} \equiv q \pmod{p}$ .

*Proof:* Let  $X$  and  $Y$  be indeterminants; we work in the polynomial ring  $(\mathbb{Z}/p\mathbb{Z})[X, Y]$ . Write  $n = p^m q$  and consider

$$(X + Y)^n = ((X + Y)^{p^m})^q = (X^{p^m} + Y^{p^m})^q = \sum_{i=0}^q \binom{q}{i} (X^{p^m})^i (Y^{p^m})^{q-i}.$$

On the other hand, we have

$$(X + Y)^n = \sum_{i=0}^n \binom{n}{i} X^i Y^{n-i}.$$

and the required result follows by comparing the coefficient of  $X^{p^m} Y^{(q-1)p^m}$  in the two expressions. ■

For the proof of the Theorem, we are going to use the following:

**Proposition 3.6.3:** Let  $P$  be a Sylow  $p$ -subgroup of  $G$  and let  $Q$  be any  $p$ -subgroup of  $G$ . Then

$$N_Q(P) = Q \cap P.$$

*Proof:* By definition,  $N_Q(P) = Q \cap N_G(P)$ , so we must show that  $Q \cap N_G(P) = Q \cap P$ .

Let  $H = Q \cap N_G(P)$ . Since  $P \subseteq N_G(P)$ , it is clear that  $Q \cap P \subseteq H = Q \cap N_G(P)$ . It remains to establish the reverse inclusion. Since  $H \subseteq Q$  by definition, it only remains to prove that  $H \subseteq P$ .

For this, we first claim that  $PH$  is a  $p$ -subgroup of  $G$ . Assume for the moment that this claim has been established. Since  $PH$  contains  $P$  and since  $P$  is a  $p$ -subgroup of maximal possible order, we conclude that  $P = PH$  and hence that  $H \subseteq P$  as required.

Since  $H \subseteq N_G(P)$ , the product  $PH = \{xh \mid x \in P \text{ and } h \in H\}$  is a subgroup of  $G$ . Moreover, we know that

$$|PH| = \frac{|P||H|}{|P \cap H|};$$

see [Corollary 2.6.5](#). Since  $|P|$  and  $|H|$  are powers of  $p$ ,  $PH$  is a  $p$ -subgroup. ■

Finally, we now give:

*Proof of Sylow's Theorem:* [Proposition 3.6.2](#) shows that  $|E| \not\equiv 0 \pmod{p}$ . Thus there must be some  $X \in E$  for which the orbit  $G \cdot X$  satisfies  $|G \cdot X| \not\equiv 0 \pmod{p}$ . If  $H$  is the stabilizer in  $G$  of  $X$ , there is of course a bijection between  $G \cdot X$  and  $G/H$ . In particular,

$$|G/H| \not\equiv 0 \pmod{p}.$$

Since  $|G| = |H| \cdot |G/H|$ , conclude that  $p^m$  divides the order of  $H$ .

On the other hand, fix  $x \in X$ . We claim that  $H \subseteq X \cdot x^{-1}$ . Indeed, for  $h \in H$ , since  $h$  stabilizes  $X$  we have  $hx = x'$  for some  $x' \in X$ . Then  $h = x'x^{-1} \in X \cdot x^{-1}$  as required.

Concluding, we find that  $|H| \leq |X \cdot x^{-1}| = |X| = p^m$  and thus  $|H| = p^m$ . In particular,  $H$  is a Sylow subgroup.

Now let  $H'$  be any  $p$ -subgroup of  $G$  and consider the action of  $H'$  on the quotient  $G/H$  determined by left-multiplication. Since  $|G/H| = q$  is not divisible by  $p$ , [Proposition 3.5.2](#) shows that  $(G/H)^{H'} \neq \emptyset$ . Suppose that the coset  $gH \in G/H$  is fixed by  $H'$ . We claim that

$$H' \subset gHg^{-1}.$$

Indeed, since  $gH$  is fixed by  $H'$ , we have

$$x \in H' \Rightarrow xgH = gH \Rightarrow g^{-1}xgH = H \Rightarrow g^{-1}xg \in H \Rightarrow x \in gHg^{-1}.$$

This confirms that  $H' \subseteq gHg^{-1}$ . Thus any  $p$ -subgroup of  $G$  is contained in a Sylow subgroup. This proves (b).

Applying the argument of the preceding paragraph to the case where  $H'$  is a Sylow subgroup we see that  $H' = gHg^{-1}$ ; this shows that any two Sylow subgroups are conjugate, proving (a).

To prove (c), let  $P$  be a Sylow  $p$ -subgroup. Note that  $P$  acts by conjugation on the set of all Sylow  $p$ -subgroups of  $G$ . We choose Sylow  $p$ -subgroups  $Q_1, Q_2, \dots, Q_s$  which form a system of representatives of the  $P$ -orbits for this action. We may and will take  $Q_1 = P$ .

For  $1 \leq i < s$ , we write  $\mathcal{O}_i = P \cdot Q_i = \{xQ_ix^{-1} \mid x \in P\}$  for the  $P$ -orbit of  $Q_i$ . Recall that  $\mathcal{O}_i$  is in bijection with the quotient  $P/N_P(Q_i)$  where  $N_P(Q_i)$  is the *normalizer* of  $Q_i$  in  $P$ .

For  $1 \leq i \leq s$  [Proposition 3.6.3](#) shows that  $N_P(Q_i) = Q_i \cap P$ .

In particular, it follows that  $N_P(Q_1) = P \cap P = P$  so that  $|\mathcal{O}_1| = 1$ . For all  $2 \leq i \leq s$  we have  $P \neq Q_i$  so that  $N_P(Q_i) = Q_i \cap P \subsetneq P$ . Thus  $|\mathcal{O}_i| = [P : Q_i \cap P] > 1$  so that

$$|\mathcal{O}_i| \equiv 0 \pmod{p}.$$

Finally, the number  $r$  of Sylow  $p$ -subgroups satisfies

$$r = \sum_{i=1}^s |\mathcal{O}_i| = 1 + \sum_{i=2}^s |\mathcal{O}_i| \equiv 1 \pmod{p}$$

which proves the first assertion of (c). The second assertion of (c) follows since

$$r = [G : N_G(P)]$$

and since  $P \subseteq N_G(P)$ . ■