

Graduate Algebra

Definition 2.3.1

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	11
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	23
3.5. p -groups	24
4. Week 4 [2025-09-22]	27
4.1. Sylow subgroups	27
4.2. Applications of Sylow's Theorem	29
4.3. Rings	33
4.4. Ring homomorphisms and kernels	34
5. Week 5 [2025-09-29]	36
5.1. Quotient rings	36
5.2. Categories	38
5.3. Modules	42
5.4. Free modules	44

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:

- We usually write 1 or sometimes 1_G rather than e for the identity element of G . + we usually write x^{-1} for the inverse of $x \in G$
- 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.)
- A group is abelian if $\forall a, b \in G, ab = ba$
- 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 φ 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 φ 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 GL_n of $n \times n$ matrices with non-zero determinant, where $n = \dim_F V$ and where the operation in GL_n is given by matrix multiplication.

1.6. Cayley’s Theorem

Let Ω 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 Ω .

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 λ_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 λ 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 λ 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 λ_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 λ_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 δ_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 λ_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 λ 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 λ is trivial and thus λ 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, π_1) and (\bar{S}_2, π_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, π_1) using

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

and let

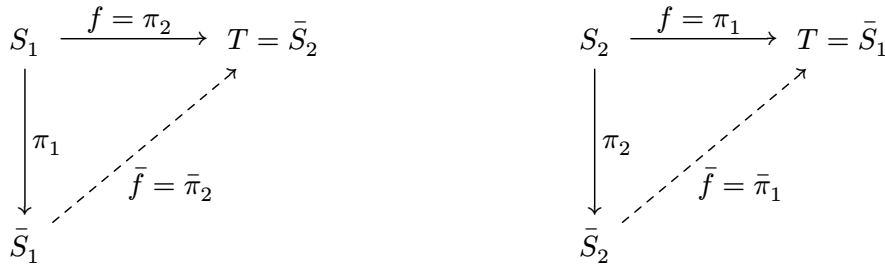
$$\bar{\pi}_1 : \bar{S}_2 \rightarrow \bar{S}_1$$

be the mapping determined by the quotient property for (\bar{S}_2, π_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 π'_1 and π'_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 π_1 and π_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}, π) .

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}, π) , 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 $\langle S \rangle = \langle s_1, s_2, \dots, s_n \rangle$.

- b. 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 Ω be a set. An **action** of G on Ω 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 Ω is a G -space.

Proposition 2.3.2: An action of a group G on a set Ω 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 Ω given by $gx = f(g)(x)$ for each $g \in G$ and $x \in \Omega$.

Definition 2.3.3: Suppose that Ω is a G -space. The G -conjugacy relation on Ω 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 Ω is an equivalence relation.

Definition 2.3.5: Let Ω 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 Ω 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: Ω is the disjoint union of the G -orbits in Ω .

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:

- 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.
- 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 $x \in G$,

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

- 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 α , 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 π ; 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 α 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 π is surjective, it follows that $\alpha(1, -) = \text{id}$. Thus $\alpha(1, z) = z$ for each $z \in G/H$, which shows that α 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

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

Since π 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 Ω_1 and on Ω_2 . A morphism of G -sets $\varphi : \Omega_1 \rightarrow \Omega_2$ is a function φ 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 φ 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 Ω 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

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

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 γ is a morphism of G -sets, it suffices to show that $(\clubsuit) \quad \forall g, g' \text{ we have}$

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

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 γ is indeed a morphism of G -sets.

Since α_x is surjective and $\gamma \circ \pi = \alpha_x$, also γ is surjective. It only remains to see that γ 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 π is constant on H -orbits, $z = \pi(g) = \pi(gg^{-1}g') = \pi(g') = z'$. This shows that γ is injective and completes the proof. ■

Definition 2.5.4: The action of G on Ω is **transitive** if there is a single G -orbit on Ω . Equivalently, the action is transitive if the quotient Ω / \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 is 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 $x_1 x_2^{-1} \in H$. Moreover, $y_1 y_2^{-1} \in K$; since H normalizes K it follows that $x_2 y_1 y_2^{-1} x_2^{-1} \in K$.

We have now argued that $a_1 a_2^{-1}$ has the form xy for $x \in H$ and $y \in K$ so that $a_1 a_2^{-1} \in X$. 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 φ 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 $h_1 k_1 = hk$ and thus $h^{-1} h_1 = k k_1^{-1}$. Now set $x = h^{-1} h_1 = k k_1^{-1} \in H \cap K$ and observe that $(h_1, k_1) = \gamma(x)$. This shows that γ is surjective. To see that γ 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 γ is injective and the proof of a. is complete.

Now, the mapping φ 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 φ 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, σ identifies with an n -cycle and τ 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, σ has order n and τ 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 σ has order n and τ 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 σ^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 φ 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 φ 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 φ is injective. The remaining assertion follows from the definition of φ . ■

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 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 Inn_x is an *automorphism* of G .
- Finally, (\blacklozenge) shows that 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 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 $\mathrm{GL}_2(\mathbb{Q})$.

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 $\forall h \in H, \mathrm{Inn}_h U_{\mathbb{Q}} \subseteq U_{\mathbb{Q}}$ 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 $\mathrm{Inn}_{h(n)} U_{\mathbb{Z}} \subset U_{\mathbb{Z}}$ since for $x \in \mathbb{Z}$

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

Note however that $\mathrm{Inn}_{h(n)} U_{\mathbb{Z}}$ is a proper subset of $U_{\mathbb{Z}}$; indeed, identifying $U_{\mathbb{Z}}$ with \mathbb{Z} , the image subgroup $\mathrm{Inn}_{h(n)} U_{\mathbb{Z}}$ 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 $\mathrm{Inn}_{h(n)}^{-1} U_{\mathbb{Z}} = \mathrm{Inn}_{h(n^{-1})} U_{\mathbb{Z}} \not\subseteq U_{\mathbb{Z}}$; indeed

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

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 $\mathrm{Inn}_x K \subseteq K$ for all $x \in S$ even though H does not normalize K .

Of course, if we insist that $\mathrm{Inn}_x K = K$ 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

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

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

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 φ 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

$$\varphi(g, g') = \pi_{G/N}(gg') = \pi_{G/N}(g_1h \cdot g'_1h') = \pi_{G/N}(g_1g'_1g'^{-1}_1hg'_1h') = \pi_{G/N}(g_1g'_1) = \varphi(g_1, g'_1)$$

since N a normal subgroup

$$\Rightarrow g'^{-1}_1hg'_1 \in N \Rightarrow g'^{-1}_1hg'_1h' \in N.$$

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 μ 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 π 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 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 φ 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

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

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

Finally, we check that φ 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

$$H^G = \{x \in H \mid \forall g \in G, g \cdot x = x\}$$

is a subgroup of H .

Proof: Notice that $1 \in H^G$ since 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.



4. Week 4 [2025-09-22]

4.1. 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 4.1.1 (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:

- Any two Sylow p -subgroups are conjugate by an element of G .
- Any p -subgroup of G is contained in a Sylow p -subgroup.
- 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 4.1.2: $\binom{p^m q}{p^m} \equiv q \pmod{p}$.

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. ■

Definition 4.1.3: Let G be a group and let $H \subseteq G$ be a subgroup. The **normalizer of H in G** is the subgroup

$$N_G(H) = \{g \in G \mid \text{Inn}_g H = H\};$$

it is the stabilizer of H in G for the conjugation action of G on the set of subgroups of G .

Notice that $G/N_G(H)$ is in bijection with the set of all conjugates $\{gHg^{-1} \mid g \in G\}$.

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

Proposition 4.1.4: 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 4.1.2](#) 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

$$hx = x' \text{ for some } x' \in X.$$

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 4.1.4](#) 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 $P \subseteq N_G(P)$. ■

For a finite group G and a prime number p , write $n_p = n_p(G)$ for the number of p -Sylow subgroups of G (this is the number r from [Theorem 4.1.1](#)).

Corollary 4.1.5:

Let $P \in \text{Syl}_p(G)$. Then P is normal if and only if $n_p = 1$.

Proof: Indeed, P is normal if and only if $\text{Inn}_G P = P$. Since all p -Sylow subgroups are conjugate, the result is immediate. ■

4.2. Applications of Sylow's Theorem

Definition 4.2.1:

Let G be a group. A subgroup H of G is **characteristic** if for every automorphism $\varphi : G \rightarrow G$, we have $\varphi(H) = H$.

A characteristic subgroup H is always normal, since H is invariant under all the inner automorphisms Inn_g for $g \in G$.

Example 4.2.2:

For a prime number p , let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$; we may identify the group G with the quotient of $\mathbb{Z} \times \mathbb{Z}$ by the subgroup $N = \langle (p, 0), (0, p) \rangle$. Write $e = (1, 0) + N$ and $f = (0, 1) + N$ so that $e, f \in G$ are elements of order p and

$$G = \langle e, f \rangle = \langle e \rangle + \langle f \rangle \text{ and } \langle e \rangle \cap \langle f \rangle = \{0\}.$$

Since G is commutative, $H = \langle e \rangle$ is a normal subgroup of G . But H is not characteristic in G . Indeed, the automorphism $(a, b) \mapsto (b, a)$ of $\mathbb{Z} \times \mathbb{Z}$ induces an automorphism φ of $G = (\mathbb{Z} \times \mathbb{Z})/N$ for which

$$\varphi(e) = f \text{ and } \varphi(f) = e.$$

Thus $\varphi(H) \neq H$.

Definition 4.2.3:

A group G is **simple** if for any normal subgroup $N \subseteq G$, either $N = \{1\}$ or $N = G$.

Any group of prime order is simple. Below we are going to find the first example of a non-abelian simple group.

Throughout the remainder of this section, G denotes a finite group.

For a prime number p we write $n_p = n_p(G)$ for the number of p -Sylow subgroups in G , and $\text{Syl}_p = \text{Syl}_p(G)$ for the set of Sylow p -subgroups. Recall that

$$n_p \equiv 1 \pmod{p} \text{ and } p \mid |G/P| \text{ for } P \in \text{Syl}_p(G)$$

.

Proposition 4.2.4:

- If $n_p = 1$ for some prime p , then $P \in \text{Syl}_p(G)$ is characteristic – and in particular normal – in G .
- Suppose that $H \subseteq G$ is a normal subgroup, and suppose that $P \in \text{Syl}_p(H)$ is a normal p -Sylow subgroup of H for some prime p . Then P is a normal subgroup of G .

Proof:

- For any automorphism φ of G , $\varphi(P)$ is again a p -Sylow subgroup of G . Since $n_p = 1$, we then $\varphi(P) = P$ so that P is indeed characteristic.
- For $g \in G$, Inn_g determines an automorphism of H . Thus by (a), $\text{Inn}_g P = P$ which shows that P is normal in G .

■

Proposition 4.2.5:

Suppose that $|G| = pq$ for distinct prime numbers $p < q$.

- a. $n_q = 1$ so that G has a normal Sylow q -subgroup.
- b. If p does not divide $q - 1$ then $n_p \equiv 1 \pmod{p}$ so that G has a normal Sylow p -subgroup. In this case, G is a cyclic group.

Proof:

- a. By [Theorem 4.1.1](#) we have $n_q \equiv 1 \pmod{q}$ and $n_q \mid p$. Since $q > p$ it follows that $n_q = 1$.
- b. Again we have $n_p \equiv 1 \pmod{p}$ and $n_p \mid q$. Since q is prime, the only possibilities are $n_p = 1$ or $n_p = q$.

If $n_p = q$ then $q \equiv 1 \pmod{p}$ so that p divides $q - 1$.

If $n_p = 1$ then $G = PQ$ where P is a Sylow p -subgroup and Q is a Sylow q -subgroup. You will prove for homework that since P and Q are both normal in G , G is isomorphic to the direct product $P \times Q$. Thus

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$$

is indeed cyclic. ■

Proposition 4.2.6:

Suppose that the size of a p -Sylow subgroup of G is p . Then G contains exactly $(p - 1) \cdot n_p$ elements of order p .

Proof: Indeed, suppose that $P, Q \in \text{Syl}_p(G)$ with $P \neq Q$. Since $|P| = |Q| = p$ is prime we know that $P \cap Q = \{1\}$. Thus

$$\left| \bigcup_{P \in \text{Syl}_p} P \setminus \{1\} \right| = \sum_{P \in \text{Syl}_p} (p - 1) = n_p(p - 1).$$

■

Proposition 4.2.7:

Suppose that $|G| = 12$. Then either $n_3 = 1$ or G is isomorphic to the alternating group A_4 , and in that case, $n_2 = 1$.

Proof:

We know that $n_3 \equiv 1 \pmod{3}$ and $n_3 \mid 4$. Thus n_3 is either 1 or 4.

To complete the proof we must show that if $n_3 = 4$ then G is isomorphic to A_4 .

The group G acts by conjugation on the set $\Omega = \text{Syl}_3$ of 3-Sylow subgroups, and $|\Omega| = 4$. This action determines a group homomorphism

$$\varphi : G \rightarrow S(\Omega) = S_4.$$

The kernel K of φ consists of all $g \in G$ which normalize each Sylow 3-subgroup. In particular for $P \in \Omega$, $K \subseteq N_G(P) = P$. Since K is normal, since P is not normal, and since $|P| = 3$, we conclude that $K = \{1\}$.

Thus φ is an isomorphism from G to its image in S_4 .

Since $n_3 = 4$, [Proposition 4.2.6](#) shows that G contains exactly 8 elements of order 3. On the other hand, there are exactly 8 three-cycles in S_4 and all are contained in A_4 .

Thus the intersection of the image of φ with A_4 is a group containing at least 8 elements. Since both groups have order 12, they must coincide.

Finally, notice that $K = \langle (12)(34), (13)(24) \rangle$ is a normal 2-sylow subgroup of A_4 ; thus $n_2(A_4) = 1$.

■

Proposition 4.2.8:

Suppose that $|G| = 30$. Then $n_5 = 1$ so that G has a normal Sylow 5-subgroup.

Proof: Let $P \in \text{Syl}_5$ and $Q \in \text{Syl}_3$.

First suppose that neither P nor Q is normal in G . In that case, $n_5 = 6$ and $n_3 = 10$. By counting elements of order 3 and of order 5, it now follows from [Proposition 4.2.6](#) that

$$|G| \geq 6 \cdot 4 + 10 \cdot 2 = 44 > 30.$$

This contradiction proves that at least one of P or Q is normal in G .

Now if either P or Q is normal in G , then PQ is a subgroup of order 15. It follows from [Proposition 4.2.5](#) that any group of order 15 is cyclic. Using [Proposition 4.2.4](#) we then conclude that both P and Q are normal in G , and the result follows.

■

Proposition 4.2.9:

Suppose that $|G| = 60$. If $n_5 > 1$ then G is a simple group.

Proof: For any group of order 60, n_5 is either 1 or 6; thus we suppose $n_5 = 6$.

Let $P \in \text{Syl}_5(G)$. If $N_G(P)$ is the normalizer of P , then $|G/N_G(P)| = 6$ so that $|N_G(P)| = 10$.

We proceed by contradiction; thus, we suppose that $\{1\} \neq H \subsetneq G$ is a normal subgroup of G .

First suppose that $5 \mid |H|$. Then H contains a Sylow 5-subgroup of G ; since H is normal, H contains all six Sylow 5-subgroups of G . Counting elements of order 5 in H , it follows from [Proposition 4.2.6](#) that

$$|H| \geq 6 \cdot 4 = 24.$$

Since the only divisor d of 60 with $d \geq 24$ is $d = 30$, we conclude that $|H| = 30$. Now [Proposition 4.2.8](#) shows that H has a normal 5-Sylow subgroup $Q \in \text{Syl}_5(H)$, and [Proposition 4.2.4](#) shows that Q is normal in G . But this contradicts the assumption $n_5 > 1$.

This shows that

$$(\clubsuit) \quad G \text{ has no normal subgroup } H \text{ for which } 5 \mid |H|.$$

Thus we may suppose that $|H|$ is a divisor of $60/5 = 12$.

If $|H| = 12$, it follows from [Proposition 4.2.7](#) that G has a normal Sylow p -subgroup for either $p = 2$ or $p = 3$. In view of [Proposition 4.2.4](#), it follows that G has a normal subgroup of order 4 or 3.

If $|G| = 6$, then G has a normal Sylow 3-subgroup by [Proposition 4.2.5](#).

Thus we may suppose that $|H|$ is one of 2, 3, 4.

Write $\overline{G} = G/H$ for the quotient group, so that $\overline{G} = 30, 20$ or 15.

We claim in each case that \overline{G} has a normal subgroup Q of order 5, i.e. that $n_5(\overline{G}) = 1$.

If $|\overline{G}| = 30$ this claim follows from [Proposition 4.2.8](#). If $|\overline{G}| = 20$ note that $n_5 \mid 4$ and $n_5 \equiv 1 \pmod{5}$ shows that $n_5 = 1$. Finally, if $|\overline{G}| = 15$, then n_5 divides 3 and $n_5 \equiv 1 \pmod{5}$ again shows that $n_5 = 1$.

If $\pi : G \rightarrow \overline{G} = G/H$ is the quotient mapping, let $H_1 = \pi^{-1}(Q)$ be the inverse image of the normal subgroup Q of order 5. You will prove for homework that H_1 is a normal subgroup of G containing H ; since $H_1/H \simeq Q$ it follows that $5 \mid |H_1|$. This contradicts (\clubsuit) and completes the proof of the Proposition. ■

Corollary 4.2.10:

The alternating group A_5 is a simple group of order 60.

Proof: Indeed, the subgroups $\langle (1, 2, 3, 4, 5) \rangle$ and $\langle (1, 3, 2, 4, 5) \rangle$ are two distinct 5-Sylow subgroups of A_5 so that $n_5(A_5) > 1$. ■

4.3. Rings

Let R be a ring and recall that we only consider rings with identity.

Definition 4.3.1:

A left ideal I of R is an additive subgroup of R that is closed under multiplication on the left by elements of R .

More precisely, for each $x \in I$ and each $a \in R$, we have $ax \in I$.

Remark 4.3.2:

- a. There is an obvious related notion of right ideal.
- b. If R is commutative, then I is a left ideal if and only if I is a right ideal, and in that case we simply call I an ideal.
- c. For non-commutative R , we reserve the term ideal for an additive subgroup I which is both a left ideal and a right ideal. Sometimes we say that such an I is a two-sided ideal, for emphasis.

Let us now suppose that R is commutative.

Proposition 4.3.3:

- a. Let I and J be ideals of R . The intersection $I \cap J$ is an ideal.
- a. More generally, if I_x is an ideal of R for each x in the index set X , then $\bigcap_{x \in X} I_x$ is an ideal of R .

Proof: Since $b \Rightarrow a$, we prove b . Note that $0 \in I_x$ for each x so that the intersection is non-empty.

Let $a, b \in \bigcap_{x \in X} I_x$. We must show that $a - b$ is in the intersection. But for $x \in X$, $a, b \in I_x \Rightarrow a - b \in I_x$ so that indeed $a - b \in \bigcap_{x \in X} I_x$. ■

Proposition/Definition 4.3.4:

Let $S \subset R$ be a subset. The ideal generated by S , written $\langle S \rangle$ or RS is defined to be

$$\bigcap_{S \subseteq I} I,$$

the intersection taken over ideals of R containing S .

Proof: This intersection is an ideal by [Proposition 4.3.3](#). ■

Definition 4.3.5:

For $a \in R$, the principal ideal generated by a is the ideal $\langle \{a\} \rangle$ and is denoted Ra or $\langle a \rangle$.

4.4. Ring homomorphisms and kernels

Definition 4.4.1:

If R and S are commutative rings, a function $f : R \rightarrow S$ is a ring homomorphism provided that it is a homomorphism of additive groups and that $f(ab) = f(a)f(b)$ for every $a, b \in R$.

Proposition 4.4.2:

If $f : R \rightarrow S$ is a ring homomorphism, the kernel $\ker f$ is an ideal of R .

Proposition 4.4.3:

If I is an ideal of R , write $\pi : R \rightarrow R/I$ for the quotient homomorphism (where R/I is the quotient additive group).

Then there is a unique ring structure on the quotient group R/I with the property that quotient mapping $\pi : R \rightarrow R/I$ is a ring homomorphism.

5. Week 5 [2025-09-29]

Parts of the material to be discussed this week are covered in the text [Dummit-Foote, “Abstract Algebra”]:

- quotient rings [Dummit-Foote] §7.3, 7.4
- modules; products and direct sums [Dummit-Foote] §10.1, 10.2, 10.3
- [Dummit-Foote] doesn’t use the language of categories.

5.1. Quotient rings

In this section, R will denote a ring (with identity as always, but not necessarily commutative).

By a (two-sided) ideal of R , we mean an additive subgroup I of R that is closed under multiplication with R on the left and on the right.

More precisely: I is an ideal if $\forall x \in I, \forall r \in R, rx \in I$ and $xr \in I$.

If I is an ideal, then R/I is an additive abelian group, and the quotient mapping $\pi : R \rightarrow R/I$ can be viewed as the mapping $\pi(r) = r + I$.

Theorem 5.1.1:

Let I be a two-sided ideal of R . Then the quotient group R/I has the structure of a ring with identity where the multiplication satisfies

$$(a + I)(b + I) = ab + I \text{ for } a, b \in R.$$

In particular, the quotient mapping $\pi : R \rightarrow R/I$ is a surjective ring homomorphism. If $I \neq R$, then $1_{R/I} \neq 0_{R/I}$.

Theorem 5.1.2 (First isomorphism theorem for rings):

Let $\varphi : R \rightarrow S$ be a surjective ring homomorphism. Recall that φ induces an isomorphism of additive groups $\bar{\varphi} : R/I \rightarrow S$ for which $\bar{\varphi}(a + I) = \varphi(a)$ for $a \in R$. Then $\bar{\varphi}$ is an isomorphism of rings.

Example 5.1.3:

Let R be a commutative ring. One checks that

$$S = \left\{ \begin{pmatrix} a & d \\ 0 & b \end{pmatrix} : a, b, c \in R \right\}$$

is a subring of $\text{Mat}_3(R)$ which is not commutative if $1_R \neq 0_R$. The mapping

$$f : S \rightarrow R \times R \text{ given by } f\left(\begin{pmatrix} a & d \\ 0 & b \end{pmatrix}\right) = (a, b)$$

is a surjective ring homomorphism with kernel $K = \left\{ \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} \mid \alpha \in R \right\}$. According to the theorem, f induces an isomorphism

$$S/K \simeq R \times R.$$

(Note that K is a two-sided ideal since $K = \ker f$. On the other hand, it is easy to check directly that K is a two-sided ideal of S .)

5.2. Categories

Definition 5.2.1: A category \mathcal{C} consists of the following:

- a class $\text{Ob}(\mathcal{C})$ of objects,
- a class $\text{Mor}(\mathcal{C})$ of morphisms together with class functions

$$\text{dom} : \text{Mor}(\mathcal{C}) \rightarrow \text{Ob}(\mathcal{C}) \text{ and } \text{codom} : \text{Mor}(\mathcal{C}) \rightarrow \text{Ob}(\mathcal{C})$$

for domain and codomain.

Denote by $\text{Mor}(X, Y) = \text{Mor}_{\mathcal{C}}(X, Y)$ the subclass of $\text{Mor}(\mathcal{C})$ consisting of morphisms f in $\text{Mor}(\mathcal{C})$ with $\text{dom}(f) = X$ and $\text{codom}(f) = Y$.

- for every three objects X, Y, Z there is a binary operation

$$(f, g) \mapsto g \circ f : \text{Mor}(X, Y) \times \text{Mor}(Y, Z) \rightarrow \text{Mor}(X, Z)$$

This data is required to satisfy:

- a. *associativity*: For f in $\text{Mor}(X, Y)$, g in $\text{Mor}(Y, Z)$ and h in $\text{Mor}(Z, W)$ we have

$$(h \circ g) \circ f = h \circ (g \circ f).$$

- b. *identity*: For every object Z , there is id_Z in $\text{Mor}(Z, Z)$ such that every f in $\text{Mor}(Z, X)$ satisfies $f \circ \text{id}_Z = f$ and every g in $\text{Mor}(X, Z)$ satisfies $\text{id}_Z \circ g = g$.

Remark 5.2.2:

We often use function notation to represent morphisms – thus $f : A \rightarrow B$ denotes the morphism f in $\text{Mor}(A, B)$. Be careful, though – in general, morphisms need not be functions.

Example 5.2.3: Here are some examples of categories.

- The category **Set** of all sets, with morphisms given by functions.
- The category **Grp** of all groups, with morphisms given by group homomorphisms.
- The category **Ab** of all abelian groups, with morphisms given by group homomorphisms.
- The category **Top** of topological spaces, with morphisms given by continuous functions.
- The category **Ring** of rings with morphisms given by ring homomorphisms.

Definition 5.2.4:

Let \mathcal{C} be a category. An object I of \mathcal{C} is said to be **initial** if for each object X of \mathcal{C} there is a unique morphism in $\text{Mor}(I, X)$.

An object T of \mathcal{C} is said to be **terminal** if for each object X of \mathcal{C} there is a unique morphism in $\text{Mor}(X, T)$.

Example 5.2.5:

- The empty set is an initial object in **Set**. Every singleton set is a terminal object in **Set**.

- b. The trivial group $\{1\}$ is both an initial and a terminal object in Grp
- c. The trivial group $\{0\}$ is both an initial and a terminal object in Ab

Definition 5.2.6:

Let \mathcal{C} be a category and let X and Y in $\text{Ob}(\mathcal{C})$. Then X and Y are **isomorphic** provided that there are morphisms $f \in \text{Mor}(X, Y)$ and $g \in \text{Mor}(Y, X)$ such that $f \circ g = \text{id}_Y$ and $g \circ f = \text{id}_X$.

One says that f and g are isomorphisms between X and Y .

Proposition 5.2.7: Let \mathcal{C} be a category.

- a. If I, I' are initial objects, there is a unique isomorphism $I \rightarrow I'$.
- b. If T, T' are terminal objects, there is a unique isomorphism $T \rightarrow T'$.

Proof: We prove a; the proof of b is essentially the same..

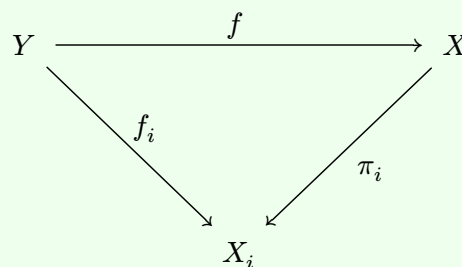
For a, since I is initial, there is a unique morphism f in $\text{Mor}(I, I')$ and since I' is initial there is a unique morphism g in $\text{Mor}(I', I)$.

Now $f \circ g$ is a morphism in $\text{Mor}(I', I')$. Since I' is initial, $\text{id}_{I'}$ is the unique morphism in $\text{Mor}(I', I')$ and we conclude that $\text{id}_{I'} = f \circ g$.

Similarly, $g \circ f$ is a morphism in $\text{Mor}(I, I)$. Since I is initial, id_I is the unique morphism in $\text{Mor}(I, I)$ and we conclude that $\text{id}_I = g \circ f$. Thus we have proved that $f : I \rightarrow I'$ is the required unique isomorphism. ■

Definition 5.2.8:

Let \mathcal{C} be a category, let I be an index set, and let X_i be an object of \mathcal{C} for each $i \in I$. A **product** of the X_i is an object X of \mathcal{C} together with morphisms $\pi_i : X \rightarrow X_i$ for $i \in I$ such that given any object Y of \mathcal{C} together with morphisms $f_i : Y \rightarrow X_i$ there is a unique morphism $f : Y \rightarrow X$ such that $f_i = \pi_i \circ f$ for each $i \in I$; i.e. the diagram



commutes for each $i \in I$.

Proposition 5.2.9:

Let \mathcal{C} be a category, let I an index set, and let X_i be objects of \mathcal{C} for $i \in I$. If a product (X, π_i) of the X_i exists in \mathcal{C} where $\pi_i : X \rightarrow X_i$ for $i \in I$, it is unique up to a unique isomorphism.

In other words, if $(X', \pi_{i'})$ is a second product in \mathcal{C} , there is a unique isomorphism $f : X \rightarrow X'$ in \mathcal{C} with the property that $\pi_i = \pi_{i'} \circ f$.

Proof: We introduce a new category \mathcal{D} depending on \mathcal{C} , I , the family X_i . An object of \mathcal{D} is an object X of \mathcal{C} together with morphisms $h_i : X \rightarrow X_i$ for each $i \in I$.

A morphism between objects (X, h_i) and (X', h'_i) of \mathcal{D} is a morphism φ in $\text{Mor}_{\mathcal{C}(X, X')}$ such that $h_i = h'_i \circ \varphi$; i.e. the diagram

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ & \searrow h_i & \swarrow h'_i \\ & X_i & \end{array}$$

commutes for each $i \in I$.

One checks that \mathcal{D} is a category. It is then clear that to give a terminal object in \mathcal{D} is the same as to give a product of the X_i in \mathcal{C} . Thus the uniqueness follows from [Proposition 5.2.7](#). ■

Remark 5.2.10:

If the objects X_i for $i \in I$ have a product in the category \mathcal{C} , we write

$$\prod_{i \in I} X_i$$

for the product, keeping in mind that the morphisms

$$\pi_j : \prod_{i \in I} X_i \rightarrow X_j$$

are part of the data determining a product.

Definition 5.2.11:

Let \mathcal{C} be a category, let I be an index set, and let X_i be an object of \mathcal{C} for each $i \in I$. A **co-product** of the X_i is an object X of \mathcal{C} together with morphisms $\gamma_i : X_i \rightarrow X$ for $i \in I$ such that given any object Y of \mathcal{C} together with morphisms $g_i : X_i \rightarrow Y$ there is a unique morphism $g : X \rightarrow Y$ such that $g_i = g \circ \gamma_i$ for each $i \in I$; i.e. the diagram

$$\begin{array}{ccc} Y & \xleftarrow{g} & X \\ & \nwarrow g_i \quad \nearrow \gamma_i & \\ & X_i & \end{array}$$

commutes for each $i \in I$.

Proposition 5.2.12:

Let \mathcal{C} be a category, let I an index set, and let X_i be objects of \mathcal{C} for $i \in I$. If a co-product (X, γ_i) of the X_i exists in \mathcal{C} where $\gamma_i : X_i \rightarrow X$, it is unique up to a unique isomorphism.

In other words, if (X', γ'_i) is a second co-product in \mathcal{C} , there is a unique isomorphism $f : X \rightarrow X'$ in \mathcal{C} with the property that $\gamma_i = f \circ \gamma'_i$.

Remark 5.2.13: If the objects X_i for $i \in I$ have a co-product in the category \mathcal{C} , we write

$$\coprod_{i \in I} X_i$$

for the co-product, keeping in mind that the morphisms

$$\gamma_j : X_j \rightarrow \coprod_{i \in I} X_i$$

are part of the data determining a co-product.

5.3. Modules

Let R be a ring.

Definition 5.3.1:

A **left R -module** M is an additive abelian group M together with an operation of scalar multiplication $R \times M \rightarrow M$ satisfying

- a. identity: $1 \cdot m = m$ for every $m \in M$.
- b. associativity: $(ab)m = a(bm)$ for every $a, b \in R$ and $m \in M$.
- c. bilinearity:
 - $(a + b)m = am + bm$ for every $a, b \in R$ and $m \in M$
 - $a(m + n) = am + an$ for every $a \in R$ and $m, n \in M$.

Remark 5.3.2:

There is a notion of right R -module M : for $r \in R$ and $m \in M$ the scalar multiplication is written $m \cdot r$ and this scalar multiplication must satisfy analogous of the conditions required for a left module. When R is commutative, any left module can be viewed as a right module – for $a \in R$ and $m \in M$ just define the right module action via $m \odot a = a \cdot m$ – and vice versa, so we may just speak of “ R -modules” in this case.

Example 5.3.3:

- a. If $R = F$ is a field, then the F -modules are precisely the F -vector spaces.
- b. Any abelian group is a \mathbb{Z} -module, and vice-versa.
- c. If R is a subring of some ring S , then S has the structure of an R -module.
- d. Any ideal I of R is an R -module (in particular, I is an R -submodule of the R -module R).

Proposition 5.3.4: The data of an R -module M is equivalent to the data of an additive abelian group M together with a ring homomorphism $R \rightarrow \text{End}_{\mathbb{Z}}(M)$, where $\text{End}_{\mathbb{Z}}(M)$ is the ring of additive endomorphisms of M .

Definition 5.3.5:

If M and N are left R -modules, a function $\varphi : M \rightarrow N$ is a homomorphism of R -modules provided that

$$\varphi(rm) = r\varphi(m) \text{ for every } r \in R \text{ and every } m \in M.$$

Remark 5.3.6:

- a. If $R = F$ is a field, then a homomorphism of R -modules $\varphi : M \rightarrow N$ is the same as a linear map of vector spaces.

- b. If A and B are abelian groups, a function $\varphi : A \rightarrow B$ is a group homomorphism if and only if it is a homomorphism of \mathbb{Z} -modules.

Definition 5.3.7: Let M be an R -module. By an R -submodule of M , we mean an additive subgroup $N \subseteq M$ such that $\forall x \in N, \forall r \in R, rx \in N$; i.e. such that $R \cdot N \subseteq N$.

Proposition 5.3.8:

Definition 5.3.9:

If R is a commutative ring, there is a category $R\text{-mod}$ whose objects are the R -modules and whose morphisms are the R -module homomorphisms.

Proposition/Definition 5.3.10:

Let I be an index set and suppose that M_i is an R -module for each $i \in I$. The **direct sum** $\bigoplus_{i \in I} M_i$ of the R -modules M_i is the set of all finitely supported functions $f : I \rightarrow \bigcup_{i \in I} M_i$ with the property that $f(j) \in M_j$ for $j \in I$.

- $\bigoplus_{i \in I} M_i$ is an R -module with pointwise addition and scalar multiplication.
- Define $\iota_j : M_j \rightarrow \bigoplus_{i \in I} M_i$ by setting $\iota_j(m)$ to be the finitely supported function on I whose support is $\{j\}$ and whose value at j is m .

For each j , the map ι_j is an R -module homomorphism.

Proposition 5.3.11:

Let I be an index set and let M_i be an R -module for each $i \in I$. Write $M = \bigoplus_{i \in I} M_i$ and $\iota_j : M_j \rightarrow M$ $j \in I$ as in [Proposition/Definition 5.3.10](#).

Then $M = \bigoplus_{i \in I} M_i$ together with the ι_j is a coproduct of the M_j in the category $R\text{-mod}$.

Recall that this means: Given any R -module N and R -module homomorphisms $f_j : M_j \rightarrow N$, there is a unique R -module homomorphism

$F : M \rightarrow N$ such that $f_j = F \circ \iota_j$.

$$\begin{array}{ccc}
 M = \bigoplus_{i \in I} M_i & \xrightarrow{F} & N \\
 & \nwarrow \iota_j \quad \nearrow f_j & \\
 & M_j &
 \end{array}$$

Proof: We first prove uniqueness. Consider an element

$$m \in M = \bigoplus_{i \in I} M_i.$$

Since m has finite support, we see that there are elements $m_j \in M_j$ where $m_j = 0$ for all but finitely many $j \in I$ with

$$m = \sum_{j \in I} \iota_j(m_j).$$

Now we see that

$$(\heartsuit) \quad F(m) = \sum_{j \in I} (F \circ \iota_j)(m_j) = \sum_{j \in I} f_j(m_j).$$

This proves the uniqueness once we shows that (\heartsuit) defines an R -module homomorphism. But this follows from the definition of the R -module structure on $\bigoplus_{i \in I} M_i$ and the fact that the f_j are R -module homomorphisms. ■

5.4. Free modules

Let R be a ring.

Definition 5.4.1:

Let F be a left R -module, let B be a set and let $\beta : B \rightarrow F$ be a function. Then F is a **free** left R -module on β provided that for any R -module X and any function $j : B \rightarrow X$, there is a unique R -module homomorphism $\varphi : F \rightarrow X$ such that $j = \varphi \circ \beta$.

Proposition 5.4.2:

Suppose that F is a free R -module on $\beta : B \rightarrow F$. Then the function β is injective (i.e. one-to-one).

Proof: Let $b_1, b_2 \in B$ and suppose that $b_1 \neq b_2$. We must show that $\beta(b_1) \neq \beta(b_2)$. To this end, let $f : B \rightarrow R$ be the function defined by

$$f(b) = \begin{cases} 1 & \text{if } b = b_1 \\ 0 & \text{otherwise} \end{cases}.$$

Since F is a free R -module on β , there is an R -module homomorphism $\varphi : F \rightarrow R$ such that $\varphi \circ \beta = f$.

Then $\varphi(\beta(b_1)) = f(b_1) = 1$ while $\varphi(\beta(b_2)) = f(b_2) = 0$. Since $\varphi(\beta(b_1)) \neq \varphi(\beta(b_2))$ we must have $\beta(b_1) \neq \beta(b_2)$ as required. ■

We are going to argue that the free R -modules are precisely those R -modules which have a basis.

Recall that for a set I and an additive abelian group A , the support of a function

$$f : I \rightarrow A \text{ is given by } \text{Supp}(f) = \{i \in I \mid f(i) \neq 0_A\}.$$

Then f has **finite support** provided that $\text{Supp}(f)$ is a finite set.

Here is the definition:

Definition 5.4.3:

If M is an R -module, a function $\beta : B \rightarrow M$ for some set B is an R -**basis** M provided that the following hold:

- β is **linearly independent** i.e. if $a : B \rightarrow R$ is a finitely supported function and if

$$\sum_{b \in B} a(b)\beta(b) = 0 \text{ then } a = 0.$$

- β **spans** M ; i.e. for $x \in M$ there is a finitely supported function $a : B \rightarrow R$ such that

$$x = \sum_{b \in B} a(b)\beta(b).$$

Notice that if $\beta : B \rightarrow M$ is an R -basis then every element $x \in M$ can be written in the form

$$x = \sum_{b \in B} a(b)\beta(b)$$

for a unique finitely supported function $a : B \rightarrow R$.

Example 5.4.4:

In general, an R -module M need not have a basis. For example, for $n \in \mathbb{N}, n > 1$, the \mathbb{Z} -module $M = \mathbb{Z}/n\mathbb{Z}$ has no \mathbb{Z} -basis, since for any $x \in M, nx = 0$ but $0 \neq n \in \mathbb{Z}$. This shows that there can be no \mathbb{Z} -linearly independent function from a non-empty set to M .

Proposition 5.4.5:

Let B be a set and let $F = F(B, R)$ be the R -module consisting of all finitely supported maps $a : B \rightarrow R$. Consider the function $\beta_0 : B \rightarrow F(B, R)$ where $\beta_0(b)$ is the function

$$\beta_0(b)(b') = \begin{cases} 1 & \text{if } b = b' \\ 0 & \text{otherwise.} \end{cases}$$

- Then F is a free R -module on β_0 .
- β_0 is an R -basis for F .

Proof: For any finitely supported function $a : B \rightarrow R$ we note that

$$(\heartsuit) \quad a = \sum_{b \in B} a(b)\beta_0(b).$$

- To see that F is a free module on the indicated data, let N be an arbitrary R -module and let $\varphi : B \rightarrow N$ be any function. We must show that there is a unique R -module mapping $\Phi : F \rightarrow N$ such that

$$(*) \quad \Phi \circ \beta_0 = \varphi.$$

We first treat uniqueness. Thus we suppose that there is a linear mapping $\Phi : F \rightarrow N$ for which $\Phi \circ \beta = \varphi$.

Using (♥), the R -linearity of Φ , and the requirement (*), we see that

$$(\clubsuit) \quad \Phi(a) = \sum_{b \in B} a(b) \Phi(\beta_0(b)) = \sum_{b \in B} a(b) \varphi(b).$$

To complete the proof, it only remains to observe that the rule specified by (♣) indeed determines an R -module homomorphism; this follows from the definition of the R -module structure on $F = F(B, R)$.

- b. We first prove that β_0 is R -linearly independent. We suppose that $a : B \rightarrow R$ is a finitely supported function such that

$$\sum_{b \in B} a(b) \beta_0(b) = 0.$$

Then (♥) shows that $a = 0$; this proves the linear independence.

Finally, we show that β_0 spans $F(B, R)$. Let $a \in F(B, R)$. Then (♥) again shows that a has the required form.

■

Proposition 5.4.6:

Let B be any set, consider for $b \in B$ the R -module $M_b = R$, and let C together with $\iota_b : R \rightarrow C$ be the coproduct (direct sum) of the modules $M_b = R$ for $b \in B$.

With notation β_0 as in [Proposition 5.4.5](#), there is an R -module isomorphism

$$\Psi : C \rightarrow F(B, R)$$

such that for each $b \in B$,

$$(\Psi \circ \iota_b)(1) = \beta_0(b).$$

Theorem 5.4.7:

Let M be an R -module, let B be a set and let $\beta : B \rightarrow F$ be a function. For $b \in B$ consider the R -module homomorphism $\iota_b : R \rightarrow M$ given by $\iota_b(r) = r\beta(b)$.

The following are equivalent:

- β is an R -basis for M
- M is a free R -module on $\beta : B \rightarrow M$.
- M together with the ι_b form a co-product of the R -modules $M_b = R$.

Proof: ($a \Rightarrow b$): Let β be a basis; we show that M is free on β . Since β is a basis, we know that any $x \in M$ may be written uniquely in the form $x = \sum_{b \in B} a(b)\beta(b)$ for some $a \in F(B, R)$ where $F(B, R)$ is the R -module of all finitely supported functions $a : B \rightarrow R$.

Thus the assignment $x \mapsto a$ defines an isomorphism of R -modules $\Psi : M \rightarrow F(B, R)$; moreover, in the notation of [Proposition 5.4.5](#), we see that $\Psi \circ \beta = \beta_0$. Now the fact that M is free on β follows at once from [Proposition 5.4.5](#).

($b \Rightarrow c$): Suppose that M is free on β . We are going to argue that M together with the ι_b form a co-product of the modules $M_b = R$ in the category $R\text{-mod}$. Thus we suppose that N is any R -module and that $f_b : R \rightarrow N$ is an R -module map for each $b \in B$.

We form the function $\varphi : B \rightarrow N$ defined by $\varphi(b) = f_b(1)$.

We claim: (\spadesuit) a linear map $\Phi : M \rightarrow N$ satisfies $\Phi \circ \beta = \varphi$ if and only if it satisfies

$$\Phi \circ \iota_b = f_b \text{ for all } b \in B.$$

Indeed, from definitions we have

$$\Phi \circ \beta = \varphi \Leftrightarrow \forall b \in B, (\Phi \circ \beta)(b) = \varphi(b) \Leftrightarrow \forall b \in B, (\Phi \circ \iota_b)(1) = f_b(1).$$

Now for each $b \in B$, the R -module homomorphisms $\Phi \circ \iota_b : R \rightarrow N$ and $f_b : R \rightarrow N$ are equal if and only if they agree at $1 \in R$. This proves the claim.

Since M is free on β , there is a unique linear mapping $\Phi : M \rightarrow N$ such that $\Phi \circ \beta = \varphi$. In view of (\spadesuit) it follows that Φ is the unique linear map satisfying $\forall b \in B, \Phi \circ \iota_b = f_b$ as well. This proves that M is a coproduct of the $M_b = R$ as required.

($c \Rightarrow a$): Assume that (M, ι_b) is a co-product of the modules $M_b = R$ for $b \in B$. We must show that β is a basis.

According to [Proposition 5.4.6](#), there is an R -module homomorphism $\Psi : M \rightarrow F(B, R)$ such that

$$(\Psi \circ \iota_b)(1) = \beta_0(b)$$

where $F(B, R)$ is the R -module of finitely supported functions $B \rightarrow R$ and where β is the mapping defined in [Proposition 5.4.5](#).

For $b \in B$, observe that $\iota_{b(1)} = \beta(b) \Rightarrow \Psi(\beta(b)) = \beta_0(b)$; thus $\Psi \circ \beta = \beta_0$.

On the other hand, according to [Proposition 5.4.5](#), $F(B, R)$ is a free R -module on β_0 . Apply the defining property of a free module – see [Definition 5.4.1](#) – to the function $\beta : B \rightarrow M$ to obtain an R -module homomorphism $\Phi : F(B, R) \rightarrow M$ with the property that $\Phi \circ \beta_0 = \beta$.

We claim that the R -module homomorphisms Φ and Ψ are inverse to one another. Once this claim is established, we see that β_0 is a basis of $F(B, R)$ implies that $\beta = \Phi \circ \beta_0$ is a basis of M .

To prove the claim, first note that

$$\Phi \circ \Psi : M \rightarrow M$$

satisfies

$$\Phi \circ \Psi \circ \iota_b = \iota_b;$$

on the other hand, since M is a coproduct, id_M is the unique R -module map such that $\text{id}_M \circ \iota_b = \iota_b$. Thus $\Phi \circ \Psi = \text{id}_M$.

Finally note that

$$\Psi \circ \Phi : F(B, R) \rightarrow F(B, R)$$

satisfies

$$\Psi \circ \Phi \circ \beta_0 = \beta_0.$$

Since $F(B, R)$ is a free R -module on β_0 , $\text{id}_{F(B, R)}$ is the unique R -module map such that $\text{id}_{F(B, R)} \circ \beta_0 = \beta_0$.

Thus $\Psi \circ \Phi = \text{id}_{F(B, R)}$ as required. This completes the proof.

■