Algebraic structures

1. | Groups

Groups and subgroups

Definition 1 (Group). A *group* is a non-empty set G together with a binary operation

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1 \cdot g_2 \end{aligned}$$

satisfying the following properties:

1. Associativity:
$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad \forall g_1, g_2, g_3 \in G$$
2. Identity element:
$$\exists e \in G \text{ such that } e \cdot g = g \cdot e = g \quad \forall g \in G$$[1]
3. Inverse element:
$$\forall g \in G, \exists h \in G \text{ such that } g \cdot h = h \cdot g = e$$
We denote h by g^{-1}.

In this context we say $(G \cdot)$ is a group. If, moreover, we have $g_1 \cdot g_2 = g_2 \cdot g_1 \ \forall g_1, g_2 \in G$, we say that the group $(G, \cdot)$ is *commutative* or *abelian*[2].

Lemma 2. Let $(G, \cdot)$ be a group. Then:

1. The identity element is unique.
2. Given an element $g \in G$, $\exists! h \in G$ such that $g \cdot h = h \cdot g = e$.
3. Given $g, h \in G$ such that $g \cdot h = e$, we have $h = g^{-1}$.

Definition 3 (Subgroup). Let $(G, \cdot)$ be a group and H be a subset of G. $(H, \cdot)$ is called a *subgroup* of $(G, \cdot)$[3] if satisfies:

1. If $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$.
2. $e \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Definition 4. Let $(G, \cdot)$ be a group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. We say that $(H, \cdot)$ is *proper* if $H \neq \{e\}, G$. Otherwise we say that $(H, \cdot)$ is *improper*.

Proposition 5. Let $(G, \cdot)$ be a group and $H \neq \varnothing$ be a subset of G. Then:

$$(H, \cdot) \text{ is a subgroup} \iff h_1 \cdot h_2^{-1} \in H \quad \forall h_1, h_2 \in H$$

Proposition 6. If $(H, +)$ is a subgroup of $(\mathbb{Z}, +)$, then $\exists n \in \mathbb{Z}$ such that $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

Proposition 7. Let $(G_i, *_i)$, $i = 1, \ldots, n$, be groups. Then, the product

$$(G_1, *_1) \times \cdots \times (G_n, *_n)$$

induces a group with the operation $\cdot$ defined as

$$(g_1, \ldots, g_n) \cdot (g_1', \ldots, g_n') = (g_1 *_1 g_1', \ldots, g_n *_n g_n')$$

where $g_i, g_i' \in G_i$.

Definition 8. The *order* of a group $(G, \cdot)$ is the number of elements in its set, that is, $|G|$.

Lemma 9. Let $(G, \cdot)$ be a group and $\{(H_i, \cdot) : i \in I\}$ be a set of subgroups of $(G, \cdot)$. Then, if

$$H = \bigcap_{i \in I} H_i$$

we have that $(H, \cdot)$ is also a subgroup of $(G, \cdot)$.

Definition 10. Let $(G, \cdot)$ be a group and $X \subseteq G$ be a subset of G. The *subgroup generated* by X, $(\langle X \rangle, \cdot)$, is the smallest subgroup of $(G, \cdot)$ containing X, that is,

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

Definition 11. Let $(G, *)$ be a group, $g \in G$ and $n \in \mathbb{Z}$. We define g^n as:

$$g^n = \begin{cases} g * \overset{(n)}{\cdots} * g & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ (g^{-1}) * \overset{(|n|)}{\cdots} * (g^{-1}) & \text{if } n < 0 \end{cases}$$

Lemma 12. Let $(G, \cdot)$ be a group and $g \in G$. Then, for all $n, m \in \mathbb{Z}$ we have:

1. $g^n \cdot g^m = g^{n+m} = g^m \cdot g^n$.
2. $(g^n)^m = g^{nm} = (g^m)^n$.

Proposition 13. Let $(G, *)$ be a group and $X \subseteq G$ be a subset of G. Then:

$$\langle X \rangle = \{e\} \cup \{g_1^{\alpha_1} * \cdots * g_n^{\alpha_n} : n \in \mathbb{N}, \alpha_i \in \mathbb{Z}, g_i \in X\}$$

Corollary 14. Let $(G, \cdot)$ be a group and $g \in G$. Then:

$$\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$$

Definition 15. Let $(G, \cdot)$ be a group and $g \in G$. A subgroup $(\langle g \rangle, \cdot)$ of $(G, \cdot)$ generated by a single element g is called a *cyclic group*.

Definition 16. Let $(G, \cdot)$ be a group and $g \in G$. The *order* of g is $\operatorname{ord}(g) := |\langle g \rangle|$.

[1] From now on, we will denote e or e_G the identity element of the group $(G, \cdot)$.
[2] Sometimes to simplify the notation and if the context is clear, we will refer to G directly as the group as well as the set.
[3] Sometimes we will denote that $(H, \cdot)$ is a subgroup of $(G, \cdot)$ by $H \leq G$.

Proposition 17. Let $(G, \cdot)$ be a group and $g \in G$. Then:

$$\operatorname{ord}(g) = \min\{i \in \mathbb{N} : g^i = e\}$$

If no such i exists, we say $\operatorname{ord}(g) = \infty$.

Corollary 18. Let $n \in \mathbb{N}$ such that $n > 1$ and $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Then:

$$\operatorname{ord}(\overline{a}) = \frac{n}{\gcd(a, n)}$$

Lemma 19. Let $(G, \cdot)$ be a group and $g \in G$ such that $\operatorname{ord}(g) = n$. Then:

1. $g^m = e \iff n \mid m$.
2. $g^m = g^{m'} \iff m = m' \mod n$.
3. If $0 \leq i \leq n$, then $g^{-i} = (g^i)^{-1} = g^{n-i}$.

Corollary 20. Let $(G_i, *_i)$, $i = 1, \ldots, n$, be groups. For $i = 1, \ldots, n$, let $g_i \in G_i$ and consider the element $g = (g_1, \ldots, g_n) \in (G_1, *_1) \times \cdots \times (G_n, *_n)$. Then:

$$\operatorname{ord}(g) = \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n))$$

Group morphisms

Definition 21 (Group morphism). Let $(G, *)$, $(H, \cdot)$ be two groups. A *group morphism* from $(G, *)$ to $(H, \cdot)$ is a function $\phi : (G, *) \to (H, \cdot)$ such that:

$$\phi(g_1 * g_2) = \phi(g_1) \cdot \phi(g_2) \quad \forall g_1, g_2 \in G$$

Lemma 22. Let $\phi : (G_1, *) \to (G_2, \cdot)$ be a morphism between $(G_1, *)$ and $(G_2, \cdot)$. Then,

1. $\phi(e_1) = e_2$.
2. $\phi(g^{-1}) = \phi(g)^{-1} \quad \forall g \in G_1$.
3. $\phi(g^n) = \phi(g)^n \quad \forall g \in G_1$ and $\forall n \in \mathbb{Z}$.

Definition 23. We say a subgroup $(H, \cdot)$ of a group $(G, \cdot)$ is *normal*, $H \trianglelefteq G$, if and only if $\forall h \in H$ and $\forall g \in G$, we have $g \cdot h \cdot g^{-1} \in H$.

Definition 24. Let $(G_1, *)$, $(G_2, \cdot)$ be two groups and $\phi : (G_1, *) \to (G_2, \cdot)$ be a group morphism. The *kernel* of ϕ is:

$$\ker \phi = \{g \in G_1 : \phi(g) = e_2\}$$

The *image* of ϕ is:

$$\operatorname{im} \phi = \{h \in G_2 : \phi(g) = h \text{ for some } g \in G_1\}$$

Proposition 25. Let $(G_1, *)$, $(G_2, \cdot)$ be two groups and $\phi : (G_1, *) \to (G_2, \cdot)$ be a group morphism. Then:

1. $(\ker \phi, *)$ is a normal subgroup of $(G_1, *)$ and $(\operatorname{im} \phi, \cdot)$ is a subgroup of $(G_2, \cdot)$.
2. Let $g, g' \in G_1$. The following statements are equivalent:
   i) $\phi(g) = \phi(g')$.
   ii) $g * g'^{-1} \in \ker \phi$.
   iii) $g'^{-1} * g \in \ker \phi$.
3. ϕ is injective if and only if $\ker \phi = \{e_1\}$.
4. ϕ is surjective if and only if $\operatorname{im} \phi = G_2$.

Definition 26. Let $(G, *)$, $(H, \cdot)$ be two groups. An *isomorphism* between $(G, *)$ and $(H, \cdot)$ is a bijective morphism between these groups. In this case, we say that $(G, *)$, $(H, \cdot)$ are *isomorphic* and we denote it by $(G, *) \cong (H, \cdot)$.

Proposition 27. Let $(G_1, \star)$, $(G_2, *)$, $(G_3, \cdot)$ be three groups and $\phi : (G_1, \star) \to (G_2, *)$, $\psi : (G_2, *) \to (G_3, \cdot)$ be two group morphisms. Then, the composition $\psi \circ \phi$ is also a group morphism.

Proposition 28. Let $(G_1, *)$, $(G_2, \cdot)$ be groups and let $\phi : (G_1, *) \to (G_2, \cdot)$ be an isomorphism. Then, $\phi^{-1} : G_2 \to G_1$ is also an isomorphism.

Theorem 29 (Classification of cyclic groups). Let $(G, \cdot)$ be a group and $g \in G$ be an element such that $\langle g \rangle = G$.

- If $|G| = \infty$, then $(G, \cdot) \cong (\mathbb{Z}, +)$. We can define the isomorphism as follows:

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (G, \cdot) \\ k &\longmapsto g^k \end{aligned}$$

- If $|G| = n$, then $(G, \cdot) \cong (\mathbb{Z}/n\mathbb{Z}, +)$. We can define the isomorphism as follows:

$$\begin{aligned} \phi : \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}, +\right) &\longrightarrow (G, \cdot) \\ \overline{k} &\longmapsto g^k \end{aligned}$$

Corollary 30. Let $(G, \cdot)$ be a group and $g \in G$ be such that $\langle g \rangle = G$. Then, all subgroups of $(G, \cdot)$ are cyclic. Moreover:

- If $|G| = \infty$, subgroups of $(G, \cdot)$ are of the form $\langle g^n \rangle$, $n \in \mathbb{N} \cup \{0\}$.
- If $|G| = n$, then there is a unique subgroup $(H, \cdot)$ of $(G, \cdot)$ for every divisor $d > 0$ of n. In fact, if $n = dq$, then $H = \langle g^q \rangle$ and $|H| = d$.

Definition 31. Let X be a set. We define the *symmetric group* $(S(X), \circ)$ as:

$$S(X) = \{f : X \to X : f \text{ is bijective}\}^4$$

Definition 32. Let $(G, \cdot)$ be a group. We define the functions:

$$\begin{aligned} \ell_g : G &\longrightarrow G \\ x &\longmapsto g \cdot r \end{aligned} \qquad \begin{aligned} r_g : G &\longrightarrow G \\ x &\longmapsto x \cdot g \end{aligned}$$

Lemma 33. Let $(G, \cdot)$ be a group. The functions ℓ_g, r_g are bijective and its inverses are $\ell_{g^{-1}}$, $r_{g^{-1}}$, respectively.

[4] Observe that if $X = \{1, \ldots, n\}$, then $S(X) = \mathrm{S}_n$.

Proposition 34. Let $(G, \cdot)$ be a group. We define the functions:

$$\begin{array}{rcl} \phi : (G, \cdot) & \longrightarrow & (S(G), \circ) \\ g & \longmapsto & \ell_g \end{array} \qquad \begin{array}{rcl} \psi : (G, \cdot) & \longrightarrow & (S(G), \circ) \\ g & \longmapsto & r_{g^{-1}} \end{array}$$

Then, ϕ and ψ are injective group morphisms.

Theorem 35 (Cayley's theorem). Let $(G, \cdot)$ be a group. Then, there is an injective morphism:

$$\phi : (G, \cdot) \longrightarrow (S(G), \circ)$$

Corollary 36. If $(G, \cdot)$ is a group with $|G| = n$, then $(G, \cdot)$ is isomorphic to a subgroup of $(\mathrm{S}_n, \circ)$.

Cosets

Definition 37. Let $(G, \cdot)$ be a finite group, $(H, \cdot)$ be a subgroup of $(G, \cdot)$ and $g_1, g_2 \in G$.

- We say $g_1 \sim g_2 \iff g_1 \cdot g_2^{-1} \in H$.
- We say $g_1 \approx g_2 \iff g_2^{-1} \cdot g_1 \in H$.

Lemma 38. Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. Then:

1. $\sim$ and $\approx$ are equivalence relations.
2. If $g \in G$, then:

   $$\begin{aligned} [g]_\sim &= H \cdot g = \{h \cdot g : h \in H\} \\ [g]_\approx &= g \cdot H = \{g \cdot h' : h' \in H\} \end{aligned}$$

   Usually we say that $H \cdot g$ are the *right cosets* in G and $g \cdot H$, the *left cosets* in G.

Definition 39. Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. We define the *set of right cosets* and the *set of left cosets*, respectively, as follows:

$$G/{\sim} = \{H \cdot g : g \in G\} \quad G/{\approx} = \{g \cdot H : g \in G\}$$

Proposition 40. Let $(G, \cdot)$ be a group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. The following statements are equivalent:

1. $H \trianglelefteq G$.
2. $g \cdot H = H \cdot g \quad \forall g \in G$.

Theorem 41 (Lagrange's theorem). Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. Then:

$$|H| \mid |G|$$

Definition 42. Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. We define the *index* of $(H, \cdot)$ in $(G, \cdot)$ as:

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

Corollary 43. Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. Then:

$$[G : H] = \left|G/{\sim}\right| = \left|G/{\approx}\right|$$

Corollary 44. Let $(G, \cdot)$ be a finite group.

1. If $g \in G$, then $\operatorname{ord}(g) \mid |G|$.
2. If $|G|$ is prime, then $(G, \cdot)$ is cyclic.
3. If $(H, \cdot)$ and $(K, \cdot)$ are subgroups of $(G, \cdot)$ and $\gcd(|H|, |K|) = 1$, then $H \cap K = \{e\}$.

Definition 45 (Quotient group). Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$ such that $H \trianglelefteq G$. We define the *quotient group* $(G/H, *)$ as

$$G/H := G/{\sim} = G/{\approx}$$

and

$$\begin{array}{rcl} * : G/H \times G/H & \longrightarrow & G/H \\ (g_1 \cdot H, g_2 \cdot H) & \longmapsto & (g_1 \cdot g_2) \cdot H \end{array}$$

Lemma 46. Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$ such that $H \trianglelefteq G$. The projection

$$\begin{array}{rcl} \pi : (G, \cdot) & \longrightarrow & \left(G/H, *\right) \\ g & \longmapsto & [g] = g \cdot H \end{array}$$

is a group morphism.

Isomorphism theorems

Theorem 47 (First isomorphism theorem). Let $(G_1, \star)$, $(G_2, \cdot)$ be groups, $\phi : (G_1, \star) \to (G_2, \cdot)$ be a group morphism and $(H, \star)$ be a subgroup of $(G_1, *)$ such that $H \trianglelefteq G_1$. If $(H, \star)$ is a subgroup of $(\ker \phi, \star)$, then there exists a unique group morphism $\psi : (G_1/H, *) \to (G_2, \cdot)$ such that the diagram of Fig. 1 is commutative, that is, $\phi = \psi \circ \pi$.

$$\begin{tikzcd} (G_1, \star) \arrow[r, "\phi"] \arrow[d, "\pi"'] & (G_2, \cdot) \\ \left(G_1/H, *\right) \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 1

The definition of ψ is $\psi([g]) = \phi(g)\ \forall g \in G_1$. In particular, if $H = \ker \phi$, then ψ is injective and therefore there is an isomorphism $\psi : (G_1/H, *) \to (\operatorname{im} \phi, \cdot)$.

Theorem 48. Let

$$\begin{array}{rcl} \phi : (\mathbb{Z}, +) & \longrightarrow & \left(\mathbb{Z}/n\mathbb{Z}, +\right) \times \left(\mathbb{Z}/m\mathbb{Z}, +\right) \\ 1 & \longmapsto & (\bar{1}, \bar{1}) \end{array}$$

be a group morphism. Then, ϕ induces a morphism $\psi : (\mathbb{Z}/nm\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +) \times (\mathbb{Z}/m\mathbb{Z}, +)$. Moreover, ψ is injective if and only if $\gcd(n, m) = 1$ and in this case ψ is an isomorphism.

Corollary 49. Let $n, m \in \mathbb{Z}$ be two coprime integers and $a, b \in \mathbb{Z}$. The system of congruences

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

has solutions and these are of the form $x \equiv c \mod nm$, where $c \equiv a \mod n$ and $c \equiv b \mod m$.

Definition 50. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$. We define the *products of group subsets* K, H as the sets:

$$H\cdot K=\{h\cdot k:h\in H,k\in K\}$$
$$K\cdot H=\{k\cdot h:k\in K,h\in H\}$$

Proposition 51. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\trianglelefteq G$. Then, $(H\cdot K,\cdot)$ is a subgroup of $(G,\cdot)$ and $H\cdot K=K\cdot H$.

Proposition 52. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\cap K=\{e\}$. If $H,K\trianglelefteq G$, then the function

$$\begin{aligned}(H\times K,*)&\longrightarrow(H\cdot K,\cdot)\\(h,k)&\longmapsto h\cdot k\end{aligned}$$

is an isomorphism. In particular, $\forall h\in H$ and $\forall k\in K$, $h\cdot k=k\cdot h$.

Theorem 53 (Second isomorphism theorem). Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\trianglelefteq G$. Then, $H\cap K\trianglelefteq K$ and:

$$K/H\cap K\cong H\cdot K/H$$

Corollary 54. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$. Then:

$$|H||K|=|H\cap K||H\cdot K|$$

Lemma 55. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\trianglelefteq G$ and $H\subseteq K$. Then, $H\trianglelefteq K$, $(K/H,*)$ is a subgroup of $(G/H,*)$ and moreover:

$$K/H\trianglelefteq G/H\iff K\trianglelefteq G$$

Theorem 56 (Correspondence theorem). Let $(G,\cdot)$ be a group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$ such that $H\trianglelefteq G$. Then, there is a bijection ϕ from the set $\mathcal{G}$ of all subgroups $(K,\cdot)$ of $(G,\cdot)$ such that $H\subseteq K$ onto the set $\mathcal{H}$ of all subgroups $(K/H,*)$ of $(G/H,*)$. More precisely, the bijection is:

$$\begin{aligned}\phi:\mathcal{G}&\longrightarrow\mathcal{H}\\K&\longmapsto K/H\end{aligned}$$

Theorem 57 (Third isomorphism theorem). Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H,K\trianglelefteq G$ and $H\subseteq K$. Then, $K/H\trianglelefteq G/H$ and:

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

Group actions

Definition 58. Let X be a set and $(G,\cdot)$ be a group. A *(left) group action* of $(G,\cdot)$ on X is a function

$$\begin{aligned}*:(G,\cdot)\times X&\longrightarrow X\\(g,x)&\longmapsto g*x\end{aligned}$$

satisfying the following properties:

1. $e*x=x$, $\forall x\in X$.
2. $(g_1\cdot g_2)*x=g_1*(g_2*x)$, $\forall x\in X$ and $\forall g_1,g_2\in G$.

A set X together with an action $*$ of $(G,\cdot)$ is usually called a *(left) G-set*.

Lemma 59. Let $(G,\cdot)$ be a group and X be a G-set. For all $g\in G$ the function

$$\begin{aligned}\ell_g:X&\longrightarrow X\\x&\longmapsto g*x\end{aligned}$$

is bijective and its inverse is $\ell_{g^{-1}}$.

Definition 60. Let $(G,\cdot)$ be a group and X be a G-set. For all $x,y\in X$, we say $x\backsim y\iff\exists g\in G:y=g*x$.

Lemma 61. The relation $\backsim$ is an equivalence relation.

Definition 62. Let $(G,\cdot)$ be a group and X be a G-set. If $x\in X$, we define the *orbit* of x as:

$$\mathcal{O}_x=[x]_\backsim=\{g*x:g\in G\}$$

Definition 63. Let $(G,\cdot)$ be a group and X be a G-set. For $x\in X$, we define the *stabilizer* of $(G,\cdot)$ with respect to x as the set:

$$G_x=\{g\in G:g*x=x\}$$

Proposition 64. Let $(G,\cdot)$ be a group and X be a G-set. For all $x\in X$, $(G_x,\cdot)$ is a subgroup of $(G,\cdot)$.

Theorem 65 (Orbit-stabilizer theorem). Let $(G,\cdot)$ be a group, X be a G-set and $x\in X$. The surjective function

$$\begin{aligned}\phi:(G,\cdot)&\longrightarrow\mathcal{O}_x\\g&\longmapsto g*x\end{aligned}$$

induces a bijective function $\psi:G/\approx\,\to\mathcal{O}_x$, where $\approx$ is the equivalence relation $g_1\approx g_2\iff g_2^{-1}\cdot g_1\in G_x$ $\forall g_1,g_2\in G$[5]. In particular, if G is finite:

$$|\mathcal{O}_x|=|[G:G_x]|$$

Corollary 66 (Orbits formula). Let $(G,\cdot)$ be a finite group and X be a finite G-set. If $x_1,\ldots,x_m$ are the elements of X and $|\mathcal{O}_{x_i}|=1$ for $i=1,\ldots,r$, then:

$$|X|=r+\sum_{i=r+1}^{m}|\mathcal{O}_{x_i}|=r+\sum_{i=r+1}^{m}|[G:G_{x_i}]|\qquad(1)$$

[5]Note that the notation $\approx$ for the equivalence relation correspond with the one defined in Theorem 37.

Applications of orbits formula

Theorem 67 (Cauchy's theorem). Let $(G, \cdot)$ be a finite group of order n and p be a prime number. If $p \mid n$, then $(G, \cdot)$ has an element of order p.

Corollary 68. Let p be an odd prime number. Then, the groups of order $2p$ are isomorphic to $(\mathbb{Z}/2p\mathbb{Z}, +)$ or $(\mathrm{D}_p, \circ)$[6].

Proposition 69. Let $(G, \cdot)$ be a group. The function

$$\begin{array}{rcl} (G, \cdot) \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g \cdot x \cdot g^{-1} \end{array}$$

is an action of $(G, \cdot)$ over itself. It is called the *conjugation action*.

Definition 70 (Center of a group). Let $(G, \cdot)$ be a group. We define the *center* of $(G, \cdot)$ as:

$$Z(G) = \{z \in G : z \cdot g = g \cdot z \ \forall g \in G\}$$[7]

Proposition 71. Let p be a prime number and $(G, \cdot)$ be a finite group of order p^n for some $n \geq 1$. Then, $|Z(G)| > 1$.

Lemma 72. Let $(G, \cdot)$ be a group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. Consider the application

$$\begin{array}{rcl} (H, \cdot) \times G/\approx & \longrightarrow & G/\approx \\ (h, g \cdot H) & \longmapsto & (h \cdot g) \cdot H \end{array}$$

This application defines an action of the subgroup $(H, \cdot)$ over the set $G/\approx$.

Definition 73. Let $(G, \cdot)$ be a group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. The *normalizer* of $(H, \cdot)$ in $(G, \cdot)$ is

$$N_G(H) = \{g \in G : g \cdot h \cdot g^{-1} \in H \ \forall h \in H\}$$

Lemma 74. Let $(G, \cdot)$ be a group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. Then, $(N_G(H), \cdot)$ is a subgroup of $(G, \cdot)$ containing H and, moreover, $H \trianglelefteq N_G(H)$.

Corollary 75. Let $(G, \cdot)$ be a finite group and $(H, \cdot)$ be a subgroup of $(G, \cdot)$. Then, by orbits formula applied to action defined on Theorem 72, we have:

$$[G : H] = [N_G(H) : H] + \sum_{|\mathcal{O}_x| > 1} |\mathcal{O}_x|$$

Proposition 76. Let $(G, \cdot)$ be a group of order $n \in \mathbb{N}$, p be a prime number such that $p \mid n$ and $(H, \cdot)$ be a subgroup of $(G, \cdot)$ of order p^i, $i \geq 1$. Suppose $p \mid [G : H]$. Then, $p \mid [N_G(H) : H]$.

Sylow's theorems

Corollary 77. Let $(G, \cdot)$ be a group of order $n \in \mathbb{N}$, p be a prime number and $(H, \cdot)$ be a subgroup of $(G, \cdot)$ such that $|H| = p^i$, $i \geq 0$. Suppose $p \mid [G : H]$. Then, there is a subgroup $(H', \cdot)$ of $(G, \cdot)$ such that $H \subset H'$ and $|H'| = p^{i+1}$. Moreover, $H \trianglelefteq H'$ and $H'/H \cong \mathbb{Z}/p\mathbb{Z}$.

Theorem 78 (First Sylow theorem). Let $(G, \cdot)$ be a finite group and p be a prime number. Suppose $|G| = p^r m$, where $r \geq 0$ and $\gcd(p, m) = 1$. Then, there is a subgroup $(K, \cdot)$ of $(G, \cdot)$ of order p^r. Moreover there is a chain of subgroups $(H_i, \cdot)$ satisfying

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = K$$

such that $H_{i+1}/H_i \cong \mathbb{Z}/p\mathbb{Z}$ for $0 \leq i < r$.

Definition 79. Let p be a prime number. A group $(G, \cdot)$ is a *p-group* if $|G| = p^r$, for some $r \in \mathbb{N}$.

Definition 80. Let p be a prime number and $(G, \cdot)$ be a group. A *Sylow p-subgroup* is a p-subgroup of $(G, \cdot)$ of maximum order.

Definition 81. Let $(G, \cdot)$ be a finite group. We say $(G, \cdot)$ is *solvable* if there is a chain of subgroups $(H_i, \cdot)$ of $(G, \cdot)$ satisfying

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

and such that the subgroups $(H_{i+1}/H_i, *)$, $0 \leq i < r$, are cyclic.

Theorem 82 (Second Sylow theorem). Let $(G, \cdot)$ be a finite group and p be a prime number. Suppose $|G| = p^r m$, where $r \geq 0$ and $\gcd(p, m) = 1$. Let $(K, \cdot)$ be a Sylow p-subgroup of $(G, \cdot)$. Then, if $(H, \cdot)$ is a subgroup of $(G, \cdot)$ of order p^i, $\exists g \in G$ such that $g \cdot H \cdot g^{-1} \subseteq K$. In particular two different Sylow p-subgroups $(K_1, \cdot)$ and $(K_2, \cdot)$ are conjugate, that is, there exists an element $g \in G$ such that $g \cdot K_1 \cdot g^{-1} = K_2$.

Theorem 83 (Third Sylow theorem). Let $(G, \cdot)$ be a finite group and p be a prime number. Suppose $|G| = p^r m$, where $r \geq 0$ and $\gcd(p, m) = 1$. Let $(K, \cdot)$ be a Sylow p-subgroup of $(G, \cdot)$ and n_p be the number of different Sylow p-subgroups of $(G, \cdot)$. Then, $n_p = [G : N_G(K)]$, $n_p \mid m$ and $n_p \equiv 1 \mod p$.

Corollary 84. Let p, q be prime numbers be such that $p < q$ and $q \not\equiv 1 \mod p$. If $(G, \cdot)$ is a group of order pq, then $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Examples of groups

Let $n \in \mathbb{N}$ and p be a prime number.

- $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
- $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

[6] See the examples at the end of this section.

[7] Note that, by Eq. (1), if we consider the conjugation action we have:

$$|G| = |Z(G)| + \sum_{|\mathcal{O}_x| > 1} |\mathcal{O}_x|$$

- $(\mathrm{S}_n, \circ)$
- $(\mathrm{A}_n, \circ)$, where $\mathrm{A}_n = \{\sigma \in \mathrm{S}_n : \operatorname{sgn}(\sigma) = 1\}$. This group is called the *alternating group*. Note that $|\mathrm{A}_n| = \frac{\mathrm{S}_n}{2} = \frac{n!}{2}$.
- $(\mathrm{GL}_n(\mathbb{A}), \cdot)$, where $\mathrm{GL}_n(\mathbb{A}) = \{\mathbf{M} \in \mathcal{M}_n(\mathbb{A}) : \mathbf{M} \text{ is invertible}\}$ and $\mathbb{A} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.
- $(\mathrm{SL}_n(\mathbb{A}), \cdot)$, where $\mathrm{SL}_n(\mathbb{A}) = \{\mathbf{M} \in \mathrm{GL}_n(\mathbb{A}) : \det \mathbf{M} = 1\}$ and $\mathbb{A} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.
- $(\mathrm{D}_n, \circ)$, where D_n is the set of rotations and reflections that leave invariant the regular polygon of n vertices centered at origin. It can be seen that $\mathrm{D}_n = \langle r, s : \operatorname{ord}(r) = n, \operatorname{ord}(s) = 2, r \circ s = s \circ r^{-1}\rangle$. This group is called the *dihedral group*. Note that $|\mathrm{D}_n| = 2n$.
- $(\mathrm{Q}_8, \cdot)$, where $\mathrm{Q}_8 = \langle a, b : \operatorname{ord}(a) = \operatorname{ord}(b) = 4, b \cdot a = a^{-1} \cdot b\rangle$. This group is called the *quaternion group*. Note that $|\mathrm{Q}_8| = 8$.
- $(\mathrm{Dic}_n, \cdot)$, where $\mathrm{Dic}_n = \langle a, b : \operatorname{ord}(a) = 2n, b^2 = a^n, b^{-1} \cdot a \cdot b = a^{-1}\rangle$. This group is called the *dicyclic group*. Note that $|\mathrm{Dic}_n| = 4n$.

Classification of groups of small order

$\|G\|$	Non-isomorphic groups
1	$\{e\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, S_3
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, Q_8
9	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	$\mathbb{Z}/10\mathbb{Z}$, D_5
11	$\mathbb{Z}/11\mathbb{Z}$
12	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_6, A_4, Dic_3
13	$\mathbb{Z}/13\mathbb{Z}$
14	$\mathbb{Z}/14\mathbb{Z}$, D_7
15	$\mathbb{Z}/15\mathbb{Z}$

2. | Rings and fields

Rings, subrings and ring morphisms

Definition 85 (Ring). A *ring* is a set R equipped with two binary operations (called addition and multiplication):

$$\begin{aligned} + : R \times R &\longrightarrow R \\ (r_1, r_2) &\longmapsto r_1 + r_2 \end{aligned} \qquad \begin{aligned} \cdot : R \times R &\longrightarrow R \\ (r_1, r_2) &\longmapsto r_1 \cdot r_2 \end{aligned}$$

satisfying the following properties:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ satisfies[8]:
   i) Associativity:
   $$(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3) \quad \forall r_1, r_2, r_3 \in R$$
   ii) Identity element[9]:
   $$\exists 1 \in R \text{ such that } 1 \cdot r = r \cdot 1 = r \quad \forall r \in R$$
   iii) Commutativity:
   $$r_1 \cdot r_2 = r_2 \cdot r_1 \quad \forall r_1, r_2 \in R$$
3. Multiplication is distributive with respect to addition:
$$(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3 \quad \forall r_1, r_2, r_3 \in R$$

In this context we say $(R, +, \cdot)$ is a ring.

Definition 86. A *noncommutative ring* is a ring whose multiplication is not commutative.

Definition 87 (Field). Let $(R, +, \cdot)$ be a ring. If every nonzero element of R has a multiplicative inverse (that is, $(R, \cdot)$ is an abelian group), we say that R is a *field*.

Proposition 88. Let $(R_i, +_i, \cdot_i)$, $i = 1, \ldots, n$, be rings. Then, the product

$$(R_1, +_1, \cdot_1) \times \cdots \times (R_n, +_n, \cdot_n)$$

induces a ring with operations $+$ and $\cdot$ defined as

$$(r_1, \ldots, r_n) + (r_1', \ldots, r_n') = (r_1 +_1 r_1', \ldots, r_n +_n r_n'),$$
$$(r_1, \ldots, r_n) \cdot (r_1', \ldots, r_n') = (r_1 \cdot_1 r_1', \ldots, r_n \cdot_n r_n'),$$

where $r_i, r_i' \in R_i$.

Definition 89. Let $(R, +, \cdot)$ be a ring. We define the *set of polynomials* over the ring $(R, +, \cdot)$ as:

$$R[x] := \{r_0 + r_1 \cdot x + \cdots + r_n \cdot x^n : r_i \in R \ \forall i \text{ and } n \geq 0\}$$

Moreover, $(R[x], +, \cdot)$ is a ring.

Definition 90. A ring $(R, +, \cdot)$ is a *Boolean ring* if $r^2 = r$ $\forall r \in R$.

Lemma 91. Let $(R, +, \cdot)$ be a ring. Then:

1. The multiplicative identity element is unique.
2. $\forall r \in R$, $0 \cdot r = 0$.
3. $\forall r \in R$, $(-1) \cdot r = -r$, where -1 is the additive inverse of 1.
4. $\forall r, s \in R$, $(-r) \cdot s = -(r \cdot s)$ and $(-r) \cdot (-s) = r \cdot s$.

Definition 92 (Subring). Let $(R, +, \cdot)$ be a ring and $S \subseteq R$ be a subset of R. $(S, +, \cdot)$ is called a *subring* of $(R, +, \cdot)$ if satisfies:

1. $(S, +)$ is a subgroup of $(R, +)$.
2. $\forall s_1, s_2 \in S$, $s_1 \cdot s_2 \in S$.

[8] Some definitions state that the commutative property is not necessary to define a ring. However, in these notes we will take the definition given.
[9] It is common to denote the additive identity element as 0 and the multiplicative identity element as 1.

3. $1 \in S$.

Definition 93 (Ring morphism). Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be two rings. A *ring morphism* from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ is a function $\phi : (R, +, \cdot) \to (S, \oplus, \odot)$ such that:

1. $\phi(r_1 + r_2) = \phi(r_1) \oplus \phi(r_2) \quad \forall r_1, r_2 \in R$[10].
2. $\phi(r_1 \cdot r_2) = \phi(r_1) \odot \phi(r_2) \quad \forall r_1, r_2 \in R$.
3. $\phi(1_R) = 1_S$.

Lemma 94. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be two rings and $\phi : R \to S$ be a ring morphism. Then, knowing that $\ker \phi = \{r \in R : f(r) = 0\}$, then:

1. $(\ker \phi, +)$ is a subgroup of $(R, +)$.
2. $\forall k \in \ker \phi$ and $\forall r \in R$, $k \cdot r \in \ker \phi$.

Proposition 95. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be two rings and $\phi : R \to S$ be a ring morphism. Then:

1. $f(0) = 0$.
2. $f(-r) = -f(r)\ \forall r \in R$.
3. If $r \in R$ has a multiplicative inverse, then $f(r)$ so it has and, moreover, $f(r^{-1}) = f(r)^{-1}$.

Proposition 96. Let $(R_1, +, \cdot)$, $(R_2, \oplus, \odot)$ and $(R_3, \boxplus, \boxdot)$ be rings and $\phi : (R_1, +, \cdot) \to (R_2, \oplus, \odot)$, $\psi : (R_2, \oplus, \odot) \to (R_3, \boxplus, \boxdot)$ be two ring morphisms. Then, the composition $\psi \circ \phi$ is also a ring morphism.

Proposition 97. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be rings and let $\phi : R \to S$ be a bijective ring morphism. Then, $\phi^{-1} : S \to R$ is also a bijective ring morphism.

Ideals

Definition 98 (Ideal). Let $(R, +, \cdot)$ be a ring. A subgroup $(I, +)$ of $(R, +)$ is an *ideal* if $\forall x \in I$ and $\forall r \in R$, $x \cdot r \in I$.

Lemma 99 (Principal ideal). Let $(R, +, \cdot)$ be a ring and $a \in R$. The set

$$(a) := a \cdot R = \{a \cdot r : r \in R\}$$

is an ideal of $(R, +, \cdot)$ and it is called *principal ideal* generated by a.

Proposition 100. Let $(R, +, \cdot)$ be a nonzero ring. R is a field if and only if $(R, +, \cdot)$ has only two ideals: $\{0\}$ and R.

Definition 101. Let $(R, +, \cdot)$ be a ring. An element $r \in R$ is a *unit* if it has a multiplicative inverse. The set of units in $(R, +, \cdot)$ is denoted by R^* or $U(R)$. Moreover, $(R^*, \cdot)$ is a group called *multiplicative group* of $(R, +, \cdot)$.

Lemma 102. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be rings and $u \in R^*$. Then:

1. If $r \in R$, then $r \cdot R = r \cdot u \cdot R$.
2. If $f : (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring morphism, then $f : (R^*, +, \cdot) \to (S^*, \oplus, \odot)$ is a group morphism.

Proposition 103. Let K be a field. Then, all ideals of $K[x]$ are principal. Moreover if $I \neq \{0\}$ is an ideal of $K[x]$, there exists a monic polynomial $p(x) \in K[x]$ such that $I = p(x) \cdot K[x]$.

Proposition 104. Let $(R, +, \cdot)$ be a ring and I, J be ideals of $(R, +, \cdot)$. Then, the sets

$$I \cap J := \{x : x \in I,\ x \in J\}$$
$$I + J := \{x + y : x \in I,\ y \in J\}$$
$$I \cdot J := \left\{ \sum_{i=1}^{n} x_i y_i : n \geq 0,\ x_i \in I,\ y_i \in J \right\}$$

are all ideals. In particular $I \cap J$ is the largest ideal contained in I and J, and $I + J$ is the smallest ideal containing I and J.

Definition 105. Let $(R, +, \cdot)$ be a ring and I, J be ideals of $(R, +, \cdot)$. If $I = (a)$ and $J = (b)$ for some $a, b \in R$, then we define (a, b) as:

$$(a, b) = (a) + (b)$$

Proposition 106. Let $a, b \in \mathbb{Z}$, $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Then:

$$(a) + (b) = (d) \qquad (a) \cap (b) = (m)$$

Definition 107. A ring is *Noetherian* if all its ideals are finitely generated.

Theorem 108 (Hilbert's basis theorem). If $(R, +, \cdot)$ is a Noetherian ring, then $(R[x_1, \dots, x_n], +, \cdot)$ is a Noetherian ring.

Lemma 109. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be two rings and $\phi : (R, +, \cdot) \to (S, \oplus, \odot)$ be a ring morphism. Then:

1. $\ker \phi$ is an ideal of $(R, +, \cdot)$.
2. $\operatorname{im} \phi$ is a subring of $(S, \oplus, \odot)$.

Ideal quotient

Definition 110. Let $(R, +, \cdot)$ be a ring and I be an ideal of $(R, +, \cdot)$. For all $r_1, r_2 \in R$, we say $r_1 \sim r_2 \iff r_1 - r_2 \in I$. Since $(I, +)$ is a subgroup of $(R, +)$, $\sim$ is an equivalence relation and we denote by

$$R/_I := \{x + I : x \in R\}$$

the set of equivalence classes.

Proposition 111. Let $(R, +, \cdot)$ be a ring and I be an ideal of $(R, +, \cdot)$. Then, R/I is a ring with operations defined as:

- $\forall r_1, r_2 \in R$, $\overline{r_1} \boxplus \overline{r_2} = \overline{r_1 + r_2}$. $\overline{0}$ is the identity element with respect to this operation.

[10] That is, ϕ is a group morphism between groups $(R, +)$ and $(S, \oplus)$.

- $\forall r_1, r_2 \in R,\ \overline{r_1} \boxdot \overline{r_2} = \overline{r_1 \cdot r_2}$. $\overline{1}$ is the identity element with respect to this operation.

Moreover the projection:

$$\begin{array}{rcl} \pi : (R,+,\cdot) & \longrightarrow & \left({}^{R}\!/_{I}, \boxplus, \boxdot\right) \\ r & \longmapsto & \overline{r} \end{array}$$

is a surjective ring morphism with $\ker \pi = I$.

Corollary 112. Let $(R,+,\cdot)$ be a ring and I be an ideal of $(R,+,\cdot)$. Ideals of R/I are of the form J/I, where J is an ideal of $(R,+,\cdot)$ containing I.

Isomorphism theorems

Theorem 113 (First isomorphism theorem). Let $(R,+,\cdot)$, $(S,\oplus,\odot)$ be two rings, $\phi : (R,+,\cdot) \to (S,\oplus,\odot)$ be a ring morphism and I be an ideal such that I is a subgroup of $(\ker\phi,+)$. Then, there exists a unique ring morphism $\psi : (R/I, \boxplus, \boxdot) \to (S,\oplus,\odot)$ such that the diagram of Fig. 2 is commutative, that is, $\phi = \psi \circ \pi$.

$$\begin{tikzcd} (R,+,\cdot) \arrow[r, "\phi"] \arrow[d, "\pi"'] & (S,\oplus,\odot) \\ \left({}^{R}\!/_{I}, \boxplus, \boxdot\right) \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 2

The definition of ψ is $\psi([r]) = \phi(r)\ \forall r \in R$. In particular, if $I = \ker\phi$, then ψ is injective and therefore there is an isomorphism $\psi : R/\ker\phi \to \operatorname{im}\phi$.

Theorem 114 (Second isomorphism theorem). Let $(R,+,\cdot)$ be a ring and I, J be ideals of $(R,+,\cdot)$. Then, $(I+J)/I$ is an ideal of R/I and there is a group isomorphism

$$\phi : {}^{(I+J)}\!/_{I} \longrightarrow {}^{J}\!/_{(I \cap J)}$$

such that $\phi(a \cdot b) = \phi(a) \cdot \phi(b)\ \forall a, b \in J$.

Theorem 115 (Third isomorphism theorem). Let $(R,+,\cdot)$ be a ring and I, J be ideals of $(R,+,\cdot)$ such that $I \subseteq J$. Then, there is a ring isomorphism:

$$\left({}^{R}\!/_{I}\right)\Big/\left({}^{J}\!/_{I}\right) \cong {}^{R}\!/_{J}$$

Theorem 116 (Correspondence theorem). Let $(R,+,\cdot)$ be ring and I be an ideal of $(R,+,\cdot)$. Then, there is a bijection ϕ from the set $\mathcal{R}$ of all ideals J of $(R,+,\cdot)$ such that $I \subseteq J$ onto the set $\mathcal{I}$ of all ideals J/I of R/I. More precisely, the bijection is:

$$\begin{array}{rcl} \phi : \mathcal{R} & \longrightarrow & \mathcal{I} \\ J & \longmapsto & {}^{J}\!/_{I} \end{array}$$

[11] From now on, for simplicity, we will denote the ring $(R,+,\cdot)$ as R.

Special rings and ideals

Definition 117. A ring $R \neq \{0\}$[11] is an *integral domain* if the product of any two nonzero elements is nonzero.

Definition 118. Let R be a ring. We say $r \in R$ is a *zero divisor* if $\exists s \in R \setminus \{0\}$ such that $r \cdot s = 0$. We say $r \in R$ is not a zero divisor if $r \cdot s = 0 \implies s = 0$.

Definition 119. Let R be an integral domain. We say R is a *principal ideal domain* (*PID*) if every ideal of R is principal.

Definition 120. Let R be a ring and $P \neq R$ be an ideal of R. We say P is *prime* if $\forall a, b \in R$, we have $a \cdot b \in P \iff a \in P$ or $b \in P$.

Definition 121. Let R be a ring and $M \neq R$ be an ideal of R. We say M is *maximal* if for any ideal I of R with $M \subseteq I$, either $I = R$ or $I = M$.

Proposition 122. Let R be a ring. Then:

1. An ideal P of R is prime if and only if R/P is an integral domain.

2. An ideal M of R is maximal if and only if R/M is a field.

In particular, all maximal ideals are prime.

Definition 123. Let R be an integral domain and $a \in R \setminus \{0\}$ be a non-unit element. We say a is *irreducible* if every factorization of a contains at least one unit.

Definition 124. Let R be an integral domain and $a \in R \setminus \{0\}$ be a non-unit element. We say a is *prime* if and only if (a) is a prime ideal or, equivalently, if $b, c \in R$ are such that $a \mid b \cdot c$, then $a \mid b$ or $a \mid c$.

Proposition 125. Let R be an integral domain and $a \in R \setminus \{0\}$ be a non-unit element.

1. If a is prime, then a is irreducible.

2. If R is a PID, the following statements are equivalent:

   i) a is irreducible.

   ii) (a) is maximal.

   iii) a is prime.

Theorem 126. Let R be a ring. All ideals $I \neq R$ are contained in a maximal ideal.

Polynomial ring

Definition 127. Let R be a ring and $p(x) \in R[x]$. If $p(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_n \neq 0$, we define the *degree* of $p(x)$ as:

$$\deg p(x) = \begin{cases} n & \text{if } p(x) \neq 0 \\ -\infty & \text{if } p(x) = 0 \end{cases}$$

Proposition 128. Let R be a ring and $p(x), q(x) \in R[x]$ be polynomials with leading coefficients p_n and q_n respectively. Then:

1. $\deg(p(x) + q(x)) \leq \max\{\deg p(x), \deg q(x)\}$ and the equality holds when $\deg p(x) \neq \deg q(x)$.

2. $\deg(p(x) \cdot q(x)) \leq \deg p(x) + \deg q(x)$ and the equality holds when either p_n or q_n is not a zero divisor.

Proposition 129. Let R be a ring and $b(x), a(x) \in R[x]$ such that the leading coefficient of $b(x)$ is a unit. Then, $\exists! q(x), r(x) \in R[x]$ such that $a(x) = b(x)q(x) + r(x)$ with $\deg r(x) < \deg b(x)$.

Proposition 130 (Universal property of polynomials). Let R, S be two rings, $\phi : R \to S$ be a ring morphism and $s \in S$. Then, $\exists! \psi : R[x] \to S$ such that ψ is a ring morphism, $\psi(r) = \phi(r)\ \forall r \in R$ and $\psi(x) = s$. That is, the diagram of Fig. 3 is commutative and $\psi(x) = s$.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, hook, "i"'] & S \\ R[x] \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 3

Proposition 131 (Universal property of polynomials in several variables). Let R, S be two rings, $\phi : R \to S$ be a ring morphism and $s_1, \ldots, s_n \in S$ be not necessarily distinct elements of S. Then, $\exists! \psi : R[x_1, \ldots, x_n] \to S$ such that ψ is a ring morphism, $\psi(r) = \phi(r)\ \forall r \in R$ and $\psi(x_i) = s_i$ for $i = 1, \ldots, n$.

Corollary 132. Let R be a ring and $r \in R$. Then, the function

$$\begin{aligned} \phi_r : R[x] &\longrightarrow R \\ p(x) &\longmapsto p(r) \end{aligned}$$

is a ring morphism. Moreover $\ker \phi_r = (x - r) \cdot R[x]$ and for all $p(x) \in R[x]\ \exists q(x) \in R[x]$ such that:

$$p(x) = (x - r) \cdot q(x) + p(r)$$

Corollary 133. Let R be a ring and $r_1, \ldots, r_n \in R$. Then, the function

$$\begin{aligned} \phi : R[x_1, \ldots, x_n] &\longrightarrow R \\ p(x_1, \ldots, x_n) &\longmapsto p(r_1, \ldots, r_n) \end{aligned}$$

is a ring morphism. Moreover for all $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]\ \exists q_i(x_1, \ldots, x_n) \in R[x]$ for $i = 1, \ldots, n$ such that:

$$p(x_1, \ldots, x_n) = p(r_1, \ldots, r_n) + \sum_{i=1}^{n} (x_i - r_i) \cdot q_i(x_1, \ldots, x_n)$$

Therefore, $\ker \phi = (x_1 - r_1, \ldots, x_n - r_n)$ and consequently:

$$R[x_1, \ldots, x_n] \big/ (x_1 - r_1, \ldots, x_n - r_n) \cong R$$

Corollary 134. Let K be a field and $r_1, \ldots, r_n \in K$. Then, the ideal $(x_1 - r_1, \ldots, x_n - r_n)$ is maximal in $K[x_1, \ldots, x_n]$ and

$$K[x_1, \ldots, x_n] \big/ (x_1 - r_1, \ldots, x_n - r_n) \cong K$$

Theorem 135 (Fundamental theorem of algebra). Ideals of $\mathbb{C}[x]$ are of the form $(x - z)$, where $z \in \mathbb{C}$. That is, irreducible polynomials in $\mathbb{C}[x]$ have degree 1.

Theorem 136 (Hilbert's Nullstellensatz). Maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ are of the form $(x_1 - z_1, \ldots, x_n - z_n)$, where $z_1, \ldots, z_n \in \mathbb{C}$.

Theorem 137 (Eisenstein's criterion). Let $a(x) \in \mathbb{Z}[x] \setminus \{0\}$ be such that $a(x) = \sum_{i=0}^{n} a_i x^i$ with $\gcd(a_0, \ldots, a_n) = 1$. If there exists a primer number p such that:

- $p \mid a_i$, $i = 0, 1, \ldots, n - 1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

then $a(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Theorem 138 (General Eisenstein's criterion). Let R be an integral domain, $a(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$ and p be a prime element in R such that:

- $p \mid a_i$, $i = 0, 1, \ldots, n - 1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$.

Then, if $a(x) = b(x) \cdot c(x)$, either $\deg b(x) = 0$ or $\deg c(x) = 0$.

Unique factorization domains

Definition 139. Let R be an integral domain. We say that two elements $a, b \in R \setminus \{0\}$ are *associated* if $\exists u \in R^*$ such that $a = b \cdot u$.

Definition 140. Let R be an integral domain. We say that R is a *unique factorization domain* (*UFD*) if $\forall a \in R \setminus \{0\}$:

1. $$a = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

   where $u \in R^*$, p_i are irreducible elements of R and $\alpha_i \in \mathbb{N}\ \forall i$.

2. Such representation is unique in the sense that if $a = vq_1^{\beta_1} \cdots q_s^{\beta_s}$, where $v \in R^*$, q_i are irreducible elements of R and $\beta_i \in \mathbb{N}\ \forall i$, then $r = s$ and $\exists \sigma \in \mathrm{S}_n$ such that p_i and $q_{\sigma(i)}$ are associated and $\alpha_i = \beta_{\sigma(i)}$ for $i = 1, \ldots, r$[12].

Definition 141. Let R be an integral domain and $a, b \in R$ be such that at least one of them is nonzero. A *greatest common divisor* of a and b is an element $d \in R$ such that:

1. $d \mid a$ and $d \mid b$.
2. If d' is a common divisor of a and b, then $d' \mid d$.

Proposition 142. Let R be a UFD. Then, $\forall a, b \in R \setminus \{0\}$ there exists a greatest common divisor of a and b. Moreover such element is unique.

Proposition 143. Let R be an integral domain. Then:

1. If R is a UFD, all irreducible elements are prime.
2. If
$$up_1 \cdots p_r = vq_1 \cdots q_s$$
where $u, v \in R^*$ and both p_i and q_i are prime elements $\forall i$, then $r = s$ and $\exists \sigma \in \mathrm{S}_r$ such that p_i is associated with $q_{\sigma(i)}$ for $i = 1, \ldots, r$.

Proposition 144. Let R be an integral domain.

1. If R is a UFD, then R satisfies the *ascending chain condition on principal ideals* (*ACCP*):
If
$$a_1 \cdot R \subseteq \cdots \subseteq a_n \cdot R$$
is an ascending chain of principal ideals, then $\exists n_0 \in \mathbb{N}$ such that $a_{n_0} \cdot R = a_i \cdot R$ for $i \geq n_0$.
2. If R satisfies the ACCP, then all elements in R are product of irreducible factors.

Theorem 145. Let R be an integral domain. Then, R is UFD if and only if:

1. All irreducible elements in R are prime.
2. ACCP is satisfied.

Lemma 146. Let R be an integral domain. Let
$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$
be a chain of ideals of R. Then,
$$\bigcup_{n \in \mathbb{N}} I_n$$
is an ideal of R.

Theorem 147. Let R be a PID. Then, R is a UFD.

Corollary 148. Let $d \in \mathbb{Z} \setminus \{0\}$ such that d is square-free. Then, $\mathbb{Z}[\sqrt{d}]$ satisfies the ACCP.

Proposition 149. Let R be an integral domain. If R satisfies the ACCP, then $R[x]$ also satisfies the ACCP.

Corollary 150. Let R be a UFD. Then, $\forall n \geq 0$, all nonzero elements of $R[x_1, \ldots, x_n]$ are product of irreducible elements.

Field of fractions

Definition 151. Let R be an integral domain. Consider the set:
$$R \times (R \setminus \{0\}) = \{(a, b) : a, b \in R, b \neq 0\}$$
We define the relation $\sim$ in the following way:
$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = a_2 b_1$$
for all $(a_1, b_1), (a_2, b_2) \in R \times (R \setminus \{0\})$.

Lemma 152. The relation $\sim$ is an equivalence relation. We denote by $Q(R)$ the set of equivalence classes $R \times (R \setminus \{0\})/\sim$ and by $\frac{a}{b}$ the equivalence class $\overline{(a, b)} \in Q(R)$. $Q(R)$ is called *field of fractions* of R.

Definition 153. Let R be an integral domain. We define the sum and multiplication in $Q(R)$ as follows:

1. $\dfrac{a_1}{b_1} + \dfrac{a_2}{b_2} = \dfrac{a_1 b_2 + a_2 b_1}{b_1 b_2},\ \forall \dfrac{a_1}{b_1}, \dfrac{a_2}{b_2} \in Q(R)$
2. $\dfrac{a_1}{b_1} \cdot \dfrac{a_2}{b_2} = \dfrac{a_1 a_2}{b_1 b_2},\ \forall \dfrac{a_1}{b_1}, \dfrac{a_2}{b_2} \in Q(R)$

Theorem 154. Let R be an integral domain and consider $(Q(R), +, \cdot)$ with the operations $+$ and $\cdot$ defined above. Then:

1. $(Q(R), +, \cdot)$ is a field.
2. The function
$$\begin{aligned} i : R &\longrightarrow Q(R) \\ r &\longmapsto \tfrac{r}{1} \end{aligned}$$
is an injective ring morphism and satisfies the following property: If K is a field and $\phi : R \to K$ is an injective ring morphism, then $\exists! \psi : Q(R) \to K$ such that ψ is a ring morphism, and the diagram of Fig. 4 is commutative.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, hook, "i"'] & K \\ Q(R) \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 4

[12] Equivalently, such representation is unique in the sense that if $a = up_1 \cdots p_r = vq_1 \cdots q_s$, where $u, v \in R^*$ and p_i, q_i are irreducible elements of $R\ \forall i$, then $r = s$ and $\exists \sigma \in \mathrm{S}_n$ such that p_i and $q_{\sigma(i)}$ are associated for $i = 1, \ldots, r$.

Irreducible and prime elements in $R[x]$

Proposition 155. Let R be a UFD and $p \in R$. The following statements are equivalent:

1. p is irreducible in R.
2. p is irreducible in $R[x]$.
3. p is prime in R.
4. p is prime in $R[x]$.

Definition 156. Let R be a UFD and $a(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$. We say $p(x)$ is a *primitive polynomial* if 1 is a greatest common divisor of $a_0, \dots, a_n$.

Lemma 157 (Gauß' lemma). Let R be a UFD and $a(x), b(x) \in R[x] \setminus \{0\}$ be primitive polynomials. Then, $a(x) \cdot b(x)$ is primitive.

Lemma 158. Let R be a UFD. Then:

1. If $c_1 \cdot a(x) = c_2 \cdot b(x)$, where $c_1, c_2 \in R$, $a(x), b(x) \in R[x]$ and $b(x)$ is primitive, then $c_1 \mid c_2$.
2. If moreover $a(x)$ is also primitive, then $\exists u \in R^*$ such that $c_1 = u \cdot c_2$.

Proposition 159. Let R be a UFD and $p(x) \in R[x]$ be a primitive polynomial. The following statements are equivalent:

1. $p(x)$ is irreducible in $R[x]$.
2. $p(x)$ is irreducible in $Q(R[x])$.
3. $p(x)$ is prime in $R[x]$.
4. $p(x)$ is prime in $Q(R[x])$.

Corollary 160 (Eisenstein's criterion). Let R be a UFD, $a(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$ and p be a prime element in R such that:

- $p \mid a_i$, $i = 0, 1, \dots, n-1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$.

Then, $a(x)$ is irreducible in $Q(R)[x]$.

Theorem 161. Let R be a UFD. Then, $R[x]$ is a UFD.

Corollary 162. $\mathbb{Z}[x_1, \dots, x_n]$ and $K[x_1, \dots, x_n]$, where K is a field, are both UFD.

Examples of rings

Let $n \in \mathbb{N}$ and $d \in \mathbb{Z}$ such that d is square-free.

- $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $R[x]$, where R is a ring[13].
- $\mathcal{M}_n(K)$, where K is a field. Note that this is a non-commutative ring.
- $\mathbb{Z}[\sqrt{d}]$, where $Z[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. In particular, the set $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[\mathrm{i}]$ is called the set of *Gaußian integers*.
- $\mathbb{Q}(\sqrt{d})$, where $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$.

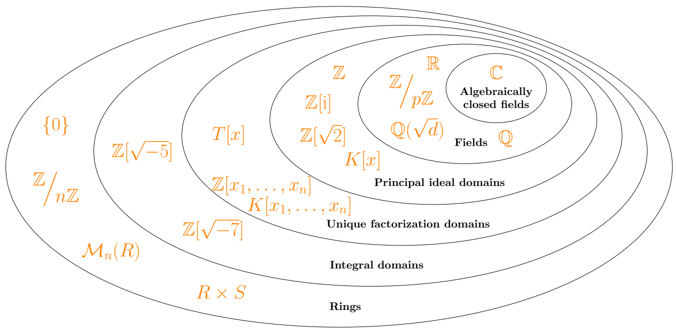

Figure 5: Inclusions of algebraic structures. Here R and S are nonzero rings, T is a UFD, K is a field, $d \in \mathbb{Z}$ such that d is square-free, $n \in \mathbb{N}$ and p is a primer number.

[13] Note that if $R = R[y]$, then $R[x] = (R[y])[x] = R[x, y]$. So the set of polynomials with several variables over a ring R is also a ring with the same operations as R.