Grupos

1. Grupos e monóides: definições básicas

Exercícios

1.1.1. Prove Proposition 1.2.

1.1.2. Let G be a semigroup. Show that G is a group iff the following conditions hold:
(i) $\exists\, e \in G\ \forall\, a \in G\ ea = a$ (left identity) and
(ii) $\forall\, a \in G\ \exists\, b \in G\ ba = e$ (left inverse).
Sugestion: Assuming (i) and (ii), first show that $a^2 = a \Rightarrow a = e$.

1.1.3. Show that the set $\{f\colon \{1,\ldots,n\} \to \{1,\ldots,n\} \mid f \text{ is bijective}\}$, with composition, is a group which is not abelian if $n > 2$ – See Example 1.7.

1.1.4. Let $\sigma \in S_n$. Show that
(a) $\exists \sigma_1, \ldots, \sigma_k$ disjoint cycles[1] s.t. $\sigma = \sigma_1 \cdots \sigma_k$.
(b) If $\sigma \in S_n$ is a cycle, then σ is a product of transpositions.

1.1.5. Let D_3 be the set of an equilateral triangle isometries (plane isometries that leave the triangle invariant) with the operation of composition. Let $\sigma, \tau \in D_3$ be, respectively, a reflexion w.r.t a symmetry axis and a rotation of $2\pi/3$. Show that each element of D_3 can be written uniquely as $\sigma^i\tau^j$, $i = 0, 1$, $j = 0, 1, 2$.

1.1.6. Let G be a group s.t. $a^2 = \mathbf{1}$ for all $a \in G$. Show that G is abelian.

1.1.7. Let G be a finite group containing an even number of elements. Show that it exists $a \in G \setminus \{\mathbf{1}\}$ s.t. $a^2 = \mathbf{1}$.

[1] $\sigma, \tau \in S_n$ are disjoint if $\{i \mid \sigma(i) \neq i\} \cap \{i \mid \tau(i) \neq i\} = \varnothing$

2. Operações definidas por passagem ao quociente

Exercícios

1.2.1. Show that $\mathbb{Z}_m$ is an abelian monoid for the operation defined by:

$$\underline{a}\,\underline{b} := \underline{ab},$$

and the *distributive property* holds:

$$\underline{a}(\underline{b} + \underline{c}) = \underline{a}\,\underline{b} + \underline{a}\,\underline{c}.$$

1.2.2. Consider the additive group $(\mathbb{Q}, +)$ and show that:
(a) the relation defined by $a \sim b \Leftrightarrow a - b \in \mathbb{Z}$ is a congruence relation, i.e., it's an equivevalence relation that preserve the group operation;
(b) the set of equivalence classes $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

1.2.3. Let p be a prime number and define $\mathbb{Z}(p^\infty) \subset \mathbb{Q}/\mathbb{Z}$ by

$$\mathbb{Z}(p^\infty) = \left\{ \left[\frac{a}{p^n} \right] \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z}, n \geq 0 \right\}.$$

Show that $\mathbb{Z}(p^\infty)$ is an infinite group with the sum of $\mathbb{Q}/\mathbb{Z}$.

3. Homomorfismos de grupos

Exercícios

1.3.1. Let $f : G \to H$ be a group homomorphism. Show that $f(\mathbf{1}_G) = \mathbf{1}_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Give an example that shows that the first property is false if G or H are monoids which are not groups.

1.3.2. Show that a group G is abelian iff $f : G \to G$, $f(x) = x^{-1}$ is an automorphism.

1.3.3. Show that $D_3 \cong S_3$.

1.3.4. Prove Proposition 3.8.

1.3.5. Show that all subgroups of $\mathbb{Z}$ are the ones in Example 3.9.

1.3.6. Show that the set $\{\sigma \in S_n \mid \sigma(n) = n\}$ is a subgroup of S_n isomorphic to S_{n-1}.

1.3.7. Let $f\colon G \to H$ be a group homomorphism and let $J < H$. Define
$$f^{-1}(J) \coloneqq \{x \in G \mid f(x) \in J\}.$$
Show that $f^{-1}(J) < G$.

1.3.8. Let G be a group and let $\mathrm{Aut}(G)$ be the set of automorphism of G. Show that $\mathrm{Aut}(G)$ is a group with operation given by composition.

1.3.9. (See Exercise 1.1.4.)
(a) Let $\sigma \in S_n$. Show that $\sigma \in A_n$ iff
$$\sigma = \sigma_1 \cdots \sigma_r, \text{ where } \sigma_i \text{ are transpositions} \quad \Rightarrow \quad r \text{ is even.}$$
(b) Show that, if $\sigma_i, \tau_j \in S_n$ are transpositions, then
$$\sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s \quad \Rightarrow \quad r \text{ and } s \text{ are both even or odd.}$$

1.3.10. Let G be a group and let $H_i < G$, $i \in I$.
(a) Prove Proposition 3.19, i.e., show that $\cap_{i\in I} H_i < G$.
(b) Show that, in general $\cup_{i\in I} H_i$ is not a group.

1.3.11. Prove Theorem 3.23.

1.3.12. (a) Let G be the group, with matrix multiplication, generated by the complex matrices
$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$
where $i^2 = -1$. Show that G is a nonabelian group with 8 elements.
Sugestion: Verify that $BA = A^3B$, so any element in Q_8 has the form A^iB^j. Verify also that $A^4 = B^4 = I \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity in G.
(b) Show that $\mathbb{H}_8 \coloneqq \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$ is a group, where $\mathbb{H}$ is the set of quaternions.
(c) Let $Q_8 = \langle a, b \mid a^2 = b^2, a^4 = 1, bab^{-1} = a^{-1}\rangle$. Show that $G \cong \mathbb{H}_8 \cong Q_8$.
Each of these groups is called *quaternion group*, which is usually denoted by Q_8.

1.3.13. Show that the additive subgroup $\mathbb{Z}(p^\infty)$ of $\mathbb{Q}/\mathbb{Z}$ (see Exercise 1.2.3) is generated by the set $\left\{\left[\dfrac{1}{p^n}\right] \mid n \in \mathbb{N}\right\}$.

4. Grupos cíclicos

Exercícios

1.4.1. (a) Show that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.
(b) Show that $\mathrm{Aut}(\mathbb{Z}_m) \cong (\mathbb{Z}_m^\times, \cdot)$, $m \in \mathbb{N}$. Sugestion: What are the generators of $\mathbb{Z}_m$?
(c) Let G be a cyclic group. Conclude that $\mathrm{Aut}(G)$ is an abelian group. Is $\mathrm{Aut}(G)$ always cyclic?

1.4.2. Prove Proposition 4.8.

1.4.3. Let G be a group and $a, b, c \in G$. Show that $|a| = |a^{-1}|$, $|ab| = |ba|$ and $|cac^{-1}| = |a|$.

1.4.4. Let G be an abelian group, $a, b \in G$ with $|a| = n$ and $|b| = m$. Show that G contains an element of order $\mathrm{lcm}(n, m)$.
Sugestion: Consider first the case when $\gcd(n, m) = 1$.

1.4.5. Let G be an abelian group of order pq with p and q relatively prime. Assuming that there exists $a, b \in G$ s.t. $|a| = p$ and $|b| = q$, show that G is cyclic.

1.4.6. Let $f : G \to H$ be a homomorphism, let $a \in G$ s.t. $f(a)$ has finite order in H. Show that either $|a|$ is infinite or $|f(a)|$ divides $|a|$.

1.4.7. (a) Consider the group $G = GL_2(\mathbb{Q})$. Show that $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ has order 4 and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ has order 3, but AB has infinite order in G.
(b) Conversely, show that the additive group[2] $\mathbb{Z}_2 \times \mathbb{Z}$ contains nonzero elements a and b of infinite order s.t. $a + b$ has finite order.

1.4.8. Prove Proposition 4.9.

1.4.9. Prove Proposition 4.10.

1.4.10. Consider again the group $\mathbb{Z}(p^\infty)$ of Exercise 1.2.3 and let $H < \mathbb{Z}(p^\infty)$. Show the following statements:
(a) Any elemnts in $\mathbb{Z}(p^\infty)$ has finite order p^n, for some $n \geq 0$.
(b) If at least one elemnet in H has order p^k and no element in H has order greater than p^k, then H is the cyclic group generated by $[\frac{1}{p^k}]$ and so $H \cong \mathbb{Z}_{p^k}$.
(c) If the set of the orders of all elements in H does not have an upper bound, then $H = \mathbb{Z}(p^\infty)$.
(d) The only proper subgroups of $\mathbb{Z}(p^\infty)$ are the cyclic groups $C_n = \langle [\frac{1}{p^n}] \rangle$, $n \in \mathbb{N}$. Moreover, $\langle 0 \rangle = C_0 < C_1 < C_2 < \cdots$.
(e) Let $x_1, x_2, \ldots$ be elements of an abelian group G s.t. $|x_1| = p$, $px_2 = x_1$, $px_3 = x_2$, $\ldots$, $px_{n+i} = x_n$, $\ldots$. The subgroup generated by x_i, with $i \geq 1$, is isomorphic to $\mathbb{Z}(p^\infty)$.
Sugestion: Verify that the map given by $x_i \mapsto [\frac{1}{p^i}]$ is well-defined and is an isomorphism.

1.4.11. Show that a group which has only finitely many subgroups is finite.

1.4.12. For an abelian group G we define $T = \{g \in G \mid |g| \text{ is finite}\}$. Show that T is a subgroup[3] of G. Is the abelian hypothesis necessary?

1.4.13. Let G be an infinite group. Show that G is cyclic iff G is isomorphic to any of its proper subgroups.

[2]If G and H are groups, the set $G \times H$ is a group for the operation defined componentwise, and identity $(\mathbf{1}_G, \mathbf{1}_H)$.
[3]This subgroup is called *torsion subgroup* of G and it is also denoted by $\mathrm{Tor}(G)$.

5. Classes laterais esquerdas, quociente por um subgrupo

Exercícios

1.5.1. Prove Proposition 5.2.

1.5.2. Prove Theorem 5.7 when G is infinite.

1.5.3. Let G be a finite group. Show that the following statements are equivalent:
 (i) $|G|$ is prime;
 (ii) $G \neq \{\mathbf{1}\}$ and G contains no proper subgroups;
 (iii) $G \cong \mathbb{Z}_p$ for some prime p.

1.5.4. Let $a \in \mathbb{Z}$ and p be a prime number s.t. $p \nmid a$. Show that $a^{p-1} \equiv 1 \pmod{p}$.

1.5.5. Show that, up to isomorphism, there are only two groups of order 4, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Sugestion: use Lagrange Theorem to conclude that a group of order 4, which is not cyclic, consists of the identity and three elements of order 2.

1.5.6. Let H, K subgroups of the group G. Show that HK is a subgroup of G iff $HK = KH$.

1.5.7. Let G be a group of order $p^k m$, where is p a prime and $\gcd(p, m) = 1$. Let $H < G$ be of order p^k and $K < G$ of order p^d, where $0 < d \leq k$, s.t. $K \not\subset H$. Show that HK is not a subgroup of G.

1.5.8. If H and K are subgroup of finite index in the group G s.t. $[G : H]$ and $[G : K]$ are relatively prime, show that $G = HK$.

6. Subgrupos normais; grupo quociente

Exercícios

1.6.1. Let $H < G$ s.t. $[G : H] = 2$. Show that $H \lhd G$.

1.6.2. Prove Proposition 6.7.

1.6.3. Show that $H \lhd G/N$ iff $H = K/N$ where $K \lhd G$ and $N < K$.

1.6.4. Let $\{N_i \mid i \in I\}$ be a family of normal subgroups in G. Show that $\cap_{i\in I} N_i \lhd G$.

1.6.5. Let $H < S_4$ be the subgroup of permutations σ s.t. $\sigma(4) = 4$. Is H normal in S_4?

1.6.6. Show that all subgroups of Q_8 are normal.

1.6.7. Let G be a finite group, let $H < G$ with $|H| = n$. If H is the unique subgroup of G with order n, show that $H \lhd G$.

1.6.8. The *dihedral group* is defined as $D_n \coloneqq \langle a, b \mid |a| = n, |b| = 2, bab = a^{-1}\rangle$. Show that
(a) $|D_n| = 2n$;
(b) $\langle a\rangle \lhd D_n$ and $D_n/\langle a\rangle \cong \mathbb{Z}_2$.

1.6.9. Let G be the subgroup S_n $(n \geq 3)$ geranerated by the permutations $\sigma = (1\ 2\ \cdots\ n)$ e

$$\tau = \begin{cases} (2\ n)(3\ n-1)\cdots(\frac{n}{2}\ \frac{n}{2}+2) & \text{if } n \text{ is even} \\ (2\ n)(3\ n-1)\cdots(\frac{n+1}{2}\ \frac{n+1}{2}+1) & \text{if } n \text{ is odd} \end{cases}$$

(a) Show that[4] $G \cong D_n$. (See the previous exercise for the definition of D_n.)
Sugestion: Consider first the cases $n = 4$ and $n = 5$, then generalize for an arbitrary n.
(b) Is G normal in S_n?

1.6.10. (a) Given examples of subgroups H and K of D_4 s.t. $H \lhd K$ and $K \lhd D_4$ but $H \ntriangleleft D_4$.
(b) If H is a cyclic subgroup of G and $H \lhd G$, show that any subgroup of H is normal in G. (Compare with the previous part.)

1.6.11. Let $H < \mathbb{Z}(p^\infty)$ s.t. $H \neq \mathbb{Z}(p^\infty)$, show that $\mathbb{Z}(p^\infty)/H \cong \mathbb{Z}(p^\infty)$.
Sugestion: If $H = \langle[\frac{1}{p^n}]\rangle$, let $x_i = [\frac{1}{p^{i+n}}]$ and use Exercise 1.4.10(e).

[4] If we consider a regular polygon with n edges with the vertices labeled consecutively from 1 to n, this description of D_n corresponds to describing the symmetries of this poligon via permutations of the vertices, namely, σ is a rotation by an angle of $\frac{2\pi}{n}$, and τ is a reflection w.r.t a "diameter".

7. Teoremas de isomorfismo

8. Produto directo e produto semidirecto de grupos

Exercícios

1.8.1. Show that $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

1.8.2. Show that $S_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

1.8.3. Let $N \lhd G$ and $K < G$ s.t. $N \cap K = \{\mathbf{1}\}$ and $NK = G$.

(a) Show that $G/N \cong K$.

(b) Is it always true that $G \cong N \times K$?

1.8.4. Let $N_1 \lhd G_1$ and $N_2 \lhd G_2$.

(a) Show that $N_1 \times N_2 \lhd G_1 \times G_2$ and

$$\frac{G_1}{N_1} \times \frac{G_2}{N_2} \cong \frac{G_1 \times G_2}{N_1 \times N_2},$$

with an isomorphism ψ defined by $\psi([g_1],[g_2]) = [(g_1,g_2)]$.

(b) Let $\widetilde{\pi}\colon G_1 \times G_2 \to G_1/N_1 \times G_2/N_2; (g_1,g_2) \mapsto ([g_1],[g_2])$. Show that $\psi \circ \widetilde{\pi}$ is the canonical projection $G_1 \times G_2 \to \frac{G_1 \times G_2}{N_1 \times N_2}$.

1.8.5. Identifying N with $N \times \{\mathbf{1}_H\}$, show that $N \lhd N \rtimes H$.

1.8.6. Let G be a group and $N \lhd G$, $H < G$ s.t. $N \cap H = \{\mathbf{1}\}$.

(a) Show that the map

$$\begin{aligned} \gamma : H &\to \operatorname{Aut}(N) \\ h &\mapsto c_h \ , \end{aligned}$$

where $c_h(n) = hnh^{-1}$ for all $n \in N$, is a group homomorphism.

(b) Show that $\psi : N \rtimes H \to G$, $\psi(n,h) = nh$, is an injective group homomorphism whose image is NH. If ψ is also surjective, i.e. $G = NH$, we say that G is the *internal semidirect product* of N and H and we write $G = N \rtimes H$.

1.8.7. Consider the subgroups $N = \langle (12)(34), (13)(24) \rangle$ and $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$ of S_4. Show that $N \lhd S_4$ and $S_4 = N \rtimes H$. Conclude that $S_4 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3$.

1.8.8. Show that Q_8 is not the internal semidirect product of proper subgroups.

9. Acções de grupos

Exercícios

1.9.1. Prove Proposition 9.4.

1.9.2. Let $\sigma = (i_1\ i_2\ \cdots\ i_r) \in S_n$ be a cycle. Show that $\tau\sigma\tau^{-1} = (\tau(i_1)\ \tau(i_2)\ \cdots\ \tau(i_r))$, for all $\tau \in S_n$.

1.9.3. Determine the conjugacy classes in S_n.
Sugestion: Use Exercise 1.9.2, and recall that any permutation is the product of disjoint cycles. Conclude that twos permutations are conjugate in S_n iff they have the same type of factorization into disjoint cycles.

1.9.4. Let G be a group. Show that $C(G) \lhd G$.

1.9.5. Show that $C(H \times K) = C(H) \times C(K)$.

1.9.6. Determine $C(Q_8)$, $C(D_4)$ and $C(D_6)$.

1.9.7. Let $n \in \mathbb{N}$ s.t. $n > 2$. Show that $C(S_n) = \langle \mathbf{1} \rangle$.

1.9.8. Show that, if $G/C(G)$ is cyclic, then G is abelian.

1.9.9. Let G be a group and $H < G$. Prove the following properties:
(a) $C_G(x) = C_G(\langle x \rangle)$ for all $x \in G$;
(b) $C_G(H) \lhd N_G(G)$;
(c) $H \lhd N_G(H)$;
(d) If $H < K < G$ and $H \lhd K$, then $K < N_G(H)$.

1.9.10. Let G be a group containing an element $a \in G$ which has exactly two conjugates. Show that G contains a proper normal subgroup $N \neq \{\mathbf{1}\}$.

1.9.11. Let G be a group. An automorphism $f \in \mathrm{Aut}(G)$ is *inner* if

$$\exists\, g \in G \quad \forall\, x \in G \quad s.t. \quad f(x) = gxg^{-1}.$$

We denote by $\mathrm{Inn}(G)$ the set of all inner automorphisms of G.
(a) Show that $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.
(b) Show that $\mathrm{Inn}(G) \cong G/C(G)$.

1.9.12. If $H < G$, show that the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

1.9.13. Give an example of an automorphism of $\mathbb{Z}_6$ which is **not** an inner automorphism.

1.9.14. Show that the center of S_4 is $C(S_4) = \{\mathbf{1}\}$ and conclude that $S_4 \cong \mathrm{Inn}(S_4)$.

1.9.15. Let G be a group containing a proper subgroup of finite index. Show that G contains a proper normal subgroup of finite index.

1.9.16. Let G be a group of order $|G| = pn$ with $p > n$, p prime, and let $H < G$ s.t. $|H| = p$. Show that $H \lhd G$.

10. Teoremas de Sylow

Exercícios

1.10.1. Let G and $N \lhd G$ s.t. N and G/N are p-groups. Show that G is a p-group.

1.10.2. Show that any group of order p^2, with p prime, is abelian.
Sugestion: Use Exercise 1.9.8.

1.10.3. Let G be a finite p-group and let be $H \lhd G$ be such that $H \neq \{\mathbf{1}\}$. Show that $H \cap C(G) \neq \{\mathbf{1}\}$.

1.10.4. Let G be a finite p-group, i.e., $|G| = p^n$. Show that G contains a normal subgroup of order p^k, for each $0 \leq k \leq n$.

1.10.5. Let G be a finite group s.t. P is a normal Sylow p-subgroup of G, and Let $f : G \to G$ be a homomorphism. Show that $f(P) < P$.

1.10.6. Let P be a Sylow p-subgroup of G
(a) Show that $N_G(N_G(P)) = N_G(P)$.
(b) Show that, if $H < G$ contains $N_G(P)$, then $N_G(H) = H$.

1.10.7. Let $D_6 = \langle a, b \mid |a| = 6, |b| = 2, bab^{-1} = a^{-1} \rangle$ be the symmetry group of a regular hexagon, where $a \in D_6$ is a rotation of $\pi/3$ and $b \in D_6$ is a reflexion
(a) Show that $\varphi(a) = (1\ 2\ 3\ 4\ 5\ 6)$ and $\varphi(b) = (1\ 2)(3\ 6)(4\ 5)$ define an injective homomorphism $\varphi : D_6 \longrightarrow S_6$ and so
$$D_6 \cong \langle (1\ 2\ 3\ 4\ 5\ 6), (1\ 2)(3\ 6)(4\ 5) \rangle < S_6.$$
(b) Find the Sylow subgroups of D_6.

1.10.8. Find the Sylow subgroups of D_{2p}, where p is an odd prime.

1.10.9. Find the Sylow 2-subgroups and 3-subgroups of S_3 and S_4.

1.10.10. Find the Sylow p-subgroups of A_5 and S_6.

1.10.11. If $|G| = p^n q$, with $p > q$ prime numbers, show that G contains a unique normal subgroup with index q.

11. Os Teoremas de Sylow como teoremas de estrutura

12. Teoria de estrutura de groups: grupos nilpotentes e grupos resolúveis

Exercícios

1.12.1. Prove Proposition 11.8.

1.12.2. Prove Proposition 12.2.

1.12.3. Let G be a group of order 45. Determine the number of Sylow p-subgroups for each prime, and justify that G is abelian, in particular, nilpotent.

1.12.4. Prove Corollary 12.10.

1.12.5. Let G be a finite nilpotent group and $N \lhd G$ s.t. $N \neq \{\mathbf{1}\}$. Show that $N \cap C(G) \neq \{\mathbf{1}\}$.

1.12.6. (a) Prove that a finite group is nilpotent iff any maximal proper subgroup of G is normal.
(b) Conclude that the index of any maximal proper subgroup is a prime number.
Sugestion: Use Exercise 1.10.6.

1.12.7. For which $n \geq 3$ is D_n a nilpotent group?

1.12.8. Prove Proposition 12.15.

1.12.9. Let $N \lhd G$. Show that $[N, G] < N$.

1.12.10. Prove Proposition 12.23.

1.12.11. Prove Proposition 12.28.

1.12.12. Compute the derived group $G^{(1)}$ in the following cases:
(a) $G = S_n$ (for $n \geq 3$),
(b) $G = A_4$,
(c) $G = D_n$.

13. Séries normais e subnormais

Exercícios

1.13.1. Show that there are no simple groups of order 20.
Sugestion: Count the Sylow p-subgroups.

1.13.2. Let G be group and $N \triangleleft G$ a normal subgroup.
(a) Show that, if N and G/N are solvable groups, G is solvable.
(b) Give an example of a group G and a subgroup $N \triangleleft G$ s.t N and G/N are nilpotent groups but G is not nilpotent.

1.13.3. Let $G = G_0 > G_1 > \cdots > G_N$ be a subnormal series of a finite group G. Show that
$$|G| = \left(\prod_{i=0}^{n-1} |G_i/G_{i+1}|\right) |G_n|.$$

1.13.4. Show that an abelian group has a composition series iff is finite.

1.13.5. Show that any solvable group with a composition series is finite.

1.13.6. Show that any group or order p^2q, where p and q are prime, is solvable.

1.13.7. Let G be the subgroup of $(\mathbb{H}^\times, \cdot)$ generated by $a = e^{\frac{\pi i}{3}}$ and $b = j$.
(a) Find the subgroups $C_k(G)$ and $G^{(k)}$, for $k \geq 1$, and decide if G is nilpotent and/or solvable.
(b) Determine a composition series for G and identify its factors.
Sugestion: Verify that $|a| = 6$, $|b| = 4$ and $bab^{-1} = a^{-1}$; justify that any element in G can be written in the form $a^r b^s$ with $r, s \geq 0$.

1.13.8. Let $G = GL_n(\mathbb{R})$ and consider the following subgroups:
$$H = \{A \in G \mid A \text{ is upper triangular}\},$$
$$K = \{A \in G \mid A \text{ is upper triangular with 1's in the diagonal}\},$$
$$D = \{A \in G \mid A \text{ is diagonal}\}.$$
Prove the following statements:
(a) K is nilpotent.
(b) $K \triangleleft H$ and $H/K \cong D$.
(c) H is solvable. Sugestion: Use the previous part and Exercise 1.13.2(a).

Anéis

1. Definições básicas

Exercícios

2.1.1. Consider the abelian group $G = \mathbb{Z} \oplus \mathbb{Z}$. Show that $\mathrm{End}(G)$ is a non commutative ring.

2.1.2. Let G be a group. Show that $\mathbb{Z}(G)$ is a ring. Give an example of a $\mathbb{Z}(G)$ containing zero divisors.

2.1.3. Let $\mathbb{H}$ the quaternion ring and recall that $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a group. What's the difference between the ring $\mathbb{H}$ and the group ring $\mathbb{R}(\mathbb{H}_8)$?

2.1.4. (Freshman's dream.) Let A be a commuatative ring with prime characteristic p. Show that $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$, for $n \geq 0$.

2.1.5. Let A be a commutative ring with prime characteristic p. Show that $f : A \to A$, $f(a) = a^p$ is a ring homomorphism.

2.1.6. An element a in a ring A is said to be *nilpotent* if $a^n = 0$ for some n. Show that in a commuatative ring A, if a and b are nilpotent, then $a + b$ is also nilpotent. Show that this result can be false if the ring is not commutative.

2. Ideais e anéis quociente

Exercícios

2.2.1. Give an example of a ring A and $a \in A$ such that $\{xay \mid x, y \in A\}$ is not an ideal.

2.2.2. Show that the set $J_k := \{A \in M_n(\mathbb{R}) \mid A^T e_i = \mathbf{0}, \text{ for } i \neq k\}$, with fixed $k = 1, \ldots, n$, is a right ideal but not a left ideal.

2.2.3. Prove Proposition 2.9, i.e., if $\{I_k \mid k \in K\}$ are (left, right) ideals in a ring A, show that $\cap_{k \in K} I_k$ is a (left, right) ideal.

2.2.4. Prove Proposition 2.15.

2.2.5. Show that a ring A is a division ring iff A contains no proper left ideal. Sugestion: Use Exercise 1.1.2.

2.2.6. Let A be a commuative ring and let N be the set of nilpotent elements in A (see Exercise 2.1.6)
(a) Show that N is an ideal.
(b) Show that A/N contains no nonzero nilpotent elements.

2.2.7. Let A be a commutative ring and let $I \subset A$ be an ideal. We define the *radical* of I by
$$\mathrm{rad}(I) = \{a \in A \mid \exists\, n \text{ s.t. } a^n \in I\}.$$
(a) Show that $\mathrm{rad}(I)$ is an ideal.
(b) Show that $\mathrm{rad}(I)$ is the intersection of all prime ideals in A that contain I.

2.2.8. Let A be a ring and let $B = M_n(A)$ be the ring of $n \times n$ matrices with entries in A. Show that $J \subset B$ is an ideal iff $J = M_n(I)$ (set of matrices with entries in I) for some ideal $I \subset A$.
Sugestion: Given J, define I as the set of elements of A which are the $(1,1)$-entry in some matrix $X \in J$ and use the *elementary matrices* $E_{i,j}$ whose (i,j)-entry is $\mathbf{1}$ and all others are $\mathbf{0}$. Verify that $E_{i,j} X E_{k,l} = x_{j,k} E_{i,l}$, where $X = [x_{ij}]$.

2.2.9. Let D be a division ring and let $A = M_n(D)$.
(a) Show that A contains no proper ideals, i.e., $\{\mathbf{0}\}$ is a maximal ideal.
Sugestion: use the previous exercise.
(b) Show that A contains zero divisors. Conclude that
(i) $S \cong S/\{\mathbf{0}\}$ is not a division ring;
(ii) $\{\mathbf{0}\}$ is a prime ideal which does not satisfy condition (2.1) in Lemma 2.25.

2.2.10. Let $f : A \to B$ be a surjective ring homomorphism and let $K = \ker f$. Prove the following statements.
(a) If $P \subset A$ is a prime ideal containing K, then $f(P) \subset B$ is a prime ideal.
(b) If $Q \subset B$ is a prime ideal, then $f^{-1}(Q) \subset A$ is a prime ideal which contains K.
(c) The following correspondence is bijective
$$\begin{aligned} \{P \subset A \text{ prime ideal s.t. } K \subset P\} &\longrightarrow \{Q \subset B \text{ prime ideal}\} \\ P &\longmapsto f(P) \end{aligned}$$
(d) Given an ideal $I \subset A$, any prime ideal in A/I is of the form P/I where $P \subset A$ is a prime ideal containing I.

2.2.11. Determine all prime ideals and maximal ideals in the ring $\mathbb{Z}_m$

2.2.12. Let A be a commutative ring and let $I \subset A$ be an ideal contained in a finite union of prime ideals, i.e., $I \subset P_1 \cup \cdots \cup P_n$, where P_i is prime. Show that $I \subset P_i$ for any $i = 1, \ldots, n$.
Sugestion: Assume that $I \cap P_j \not\subset \cup_{i \neq j} P_i$ for some j and let $a_j \in (I \cap P_j) \setminus \big(\cup_{i \neq j} P_i\big)$. Verify that $a := a_1 + a_2 a_3 \cdots a_n \in I$ but $a \notin P_1 \cup \cdots \cup P_n$.

3. Conjuntos parcialmente ordenados: lema de Zorn

4. Produto de anéis

Exercícios

2.4.1. Let A and B be rings. Show that $(A \times B)^{\times} = A^{\times} \times B^{\times}$.

2.4.2. Let A and B be rings, and let K be an ideal in $A \times B$.
- (a) Justify that $I = \{a \in A \mid (a, \mathbf{0}) \in K\}$ is an ideal in A and $J = \{b \in B \mid (\mathbf{0}, b) \in K\}$ is an ideal in B.
- (b) Given $(a, b) \in K$, show that $(a, \mathbf{0}) \in K$ and $(\mathbf{0}, b) \in K$.
- (c) Show that $K = I \times J$. So any ideal $A \times B$ is of this form.
- (d) Generalize the previous part for ideals in the product ring $A_1 \times \cdots \times A_n$.

2.4.3. Let A and B be rings, let $I \subset A$ and $J \subset B$ be ideals. Show that $(A \times B)/(I \times J) \cong (A/I) \times (B \times J)$, via a ring isomorphism.

5. Anéis Comutativos

6. Factorização em anéis comutativos

Exercícios

2.6.1. Let D be a u.f.d. and let $d \in D \setminus \{\mathbf{0}\}$. Show that there exists only a finite number of principal ideals which contain the ideal (d).

2.6.2. (Even in a integral domain, there can be irreducible elements which are not prime.) Consider the ring

$$\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$$

and the map $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ given by

$$N(m + n\sqrt{-5}) = (m + n\sqrt{-5})(m - n\sqrt{-5}) = m^2 + 5n^2 .$$

Prove the following statements:
(a) $\forall\, a, b \in \mathbb{Z}[\sqrt{-5}] \quad N(ab) = N(a)N(b)$;
(b) $N(a) = 0 \Leftrightarrow a = 0$;
(c) $a \in \mathbb{Z}[\sqrt{-5}]^{\times} \Leftrightarrow N(a) = \pm 1$;
(d) $3, 2 \pm \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.
Since $3^2 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$, conclude that the elements $3, 2\pm\sqrt{-5}$ are irreducible but not prime.

2.6.3. Determine the prime elements and the irreducible elements in $\mathbb{Z}_{15}$.

7. Factorização em domínios integrais

8. Domínios Euclidianos

Exercícios

2.8.1. Show that $\mathbb{Z}[\mathrm{i}] := \{n+m\mathrm{i} \mid n, m \in \mathbb{Z}\} \subset \mathbb{C}$ is an eucledian domain for $\varphi(n+m\mathrm{i}) = n^2+m^2$, by answering the following questions:

(a) Show that φ is a multiplicative map, i.e., $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in \mathbb{Z}[\mathrm{i}]$ and deduce property (i) in the definition.

(b) Given $k, a \in \mathbb{Z}$, with $a > 0$, show that there exists $q, r \in \mathbb{Z}$ such that $k = qa + r$, where $|r| \leq \frac{a}{2}$.

(c) Prove property (ii) where $a \in \mathbb{N}$ and $b = n + m\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$.
Sugestion: use the previous part to obtain $n = q_1 a + r_1$ and $m = q_2 a + r_2$, and consider $q := q_1 + q_2\mathrm{i}$ and $r := r_1 + r_2\mathrm{i}$.

(d) Prove property (ii) for $a, b \in \mathbb{Z}[\mathrm{i}]$.
Sugestion: if $a = x + y\mathrm{i} \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$, then $a\bar{a} = x^2 + y^2 \in \mathbb{N}$ (where $\bar{a} = x - y\mathrm{i}$) and use the previous part with $a\bar{a}$ and $b\bar{a}$.

2.8.2. Determine the units in the ring $\mathbb{Z}[\mathrm{i}]$.
Sugestion for an "efficient" solution: describe the units in $\mathbb{Z}[\mathrm{i}]$ using the application φ of the previous exercise.

2.8.3. Let A be a principal ideal commutative ring. Show that any set $X \subset A$, $X \neq \varnothing$, has a greatest common divisor.

9. Localização

Exercícios

2.9.1. Let A be a commutative ring and let S be a multiplicative subset. Show that $\frac{a}{\mathbf{1}} \in S^{-1}A$ is invertible iff $(a) \cap S \neq \varnothing$.

2.9.2. Determine $S^{-1}\mathbb{Z}_n$, for $n \geq 2$, where $S = \{\underline{a} \in \mathbb{Z}_n \mid \underline{a} \neq \underline{0},\ \underline{a} \text{ is not a zero divisor}\}$.

2.9.3. Let $A = \mathbb{Z}_6$ and $S = \{\underline{1}, \underline{2}, \underline{4}\}$. Show that S is a multiplicative set and $S^{-1}A \cong \mathbb{Z}_3$.

2.9.4. Let A be a commutative ring and S a multiplicative subset such that $S \subset A^{\times}$. Show that $\varphi_S : A \to S^{-1}A, \varphi(a) = \frac{a}{\mathbf{1}}$, is an isomorphism.

2.9.5. Show that
  (a) $\mathrm{Frac}(\mathrm{Frac}(A)) \cong \mathrm{Frac}(A)$ for any integral domain A;
  (b) $\mathrm{Frac}(k) \cong k$ for any field k.

10. Ideais de $S^{-1}A$

Exercícios

2.10.1. Prove Proposition 10.2.

2.10.2. Prove Proposition 10.3.

2.10.3. Prove Proposition 10.4.

2.10.4. Let D be a p.i.d. and let $S \subset D$ be a multiplicative set such that $0 \notin S$. Show that $S^{-1}D$ is a p.i.d.

2.10.5. Show that an integral domain D is a u.f.d. iff any nonzero prime ideal contains a principal nonzero prime ideal.
Sugestion for proving ($\Leftarrow$): First show the following statements.
(i) Let $S = D^\times \cup \{p_1 \cdots p_n \mid n \in \mathbb{N}, p_1 \ldots, p_n \in D \text{ primes}\}$. Then S is a multiplicative set such that, if $ab \in S$, then $a \in S$ and $b \in S$.
(ii) If $S \subset D$ is a multiplicative set (with $\mathbf{0} \notin S$), then for any $x \in D$ such that $(x) \cap S = \varnothing$ there exists a prime ideal $P \subset D$ such that $(x) \subset P$ and $P \cap S = \varnothing$.
Sugestion: use the caracterization of prime ideals in $S^{-1}D$.

2.10.6. Let D be a u.f.d and $S \subset D$ a multiplicative set such that $0 \notin S$. Show that $S^{-1}D$ is a u.f.d.
Sugestion: Use Exercise 2.10.5.

2.10.7. Let $p \in \mathbb{Z}$ be a prime number. What's the relation between the quotient ring $\mathbb{Z}_p = \mathbb{Z}/(p)$ and the localization $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$, where $S = \mathbb{Z} \setminus (p)$?

2.10.8. Prove Proposition 10.10.

2.10.9. Let $p \in \mathbb{Z}$ be a prime number. Show that $A = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ is a local ring.

2.10.10. Let $f : A \to B$ be a non-zero ring homomorphism. Show that, if A is local, then $f(A)$ is also local.

2.10.11. Let A be a commutative ring and let N be the ideal of the nilpotent elements in A (see Exercise 2.2.6). Show that N is the intersection of all prime ideals in A.
Sugestion to prove that N contains the intersection of all prime ideals: Given $r \in A \setminus N$, find a prime ideal $P \subset A$ such that $r \notin P$ by considering the localization $S^{-1}A$, where $S = \{r^n \mid n \in \mathbb{N}_0\}$.

11. Anéis de polinómios

Exercícios

2.11.1. Let $A = M_2(\mathbb{Z})$.
(a) Given any matrix $M \in A$, show that $(x+M)(x-M) = x^2 - M^2$ in $A[x]$.
(b) Give an example of matrices $M, N \in A$ such that $(N+M)(N-M) \neq N^2 - M^2$.
Conclude that Proposition 11.16 might be false if the rings are not commutative.

2.11.2. (Universal property of the polinimial ring $A[x_1, \dots, x_n]$, when A is not necessarely commutative.) Let A, B be rings and $\varphi : A \to B$ be a ring homomorphism such that

$$\exists\, b_1, \dots, b_n \in B \quad \forall i, j \quad \forall\, a \in A \quad b_i b_j = b_j b_i \quad \text{and} \quad \varphi(a) b_i = b_i \varphi(a)\ .$$

(a) Show that there exists a unique homomorphism $\bar{\varphi} : A[x_1, \dots, x_n] \to B$ such that $\bar{\varphi}|_A = \varphi$ and $\bar{\varphi}(x_i) = b_i$.
(b) Show that the previous property determines the ring $A[x_1, \dots, x_n]$ up to isomorphism.

2.11.3. Let A be a commutative ring. If $f = a_n x^n + \cdots + a_1 x + a_0$ is a zero divisor in $A[x]$, show that there is $b \in A \setminus \{0\}$ such that $ba_n = \cdots = ba_0 = 0$.

2.11.4. Let A be a commutative ring and let S be multiplicative subset of A. Show that $S^{-1}(A[x]) \cong (S^{-1}A)[x]$.

2.11.5. Let A be a commuative ring and $a \in A$. Show that $ax + 1$ is invertible in $A[x]$ iff a is nilpotent in A.

12. Séries formais

Exercícios

2.12.1. Let A be a ring. Show that, for $n \geq 1$,
(a) $M_n(A)[x] \cong M_n\big(A[x]\big)$;
(b) $M_n(A)[[x]] \cong M_n\big(A[[x]]\big)$.

2.12.2. Justify the following statements:
(a) The polinomial $x + 1$ is a unit in $\mathbb{Z}[[x]]$, but not in $\mathbb{Z}[x]$.
(b) the polinomial $x^2 + 3x + 2$ is irreducible in $\mathbb{Z}[[x]]$, but not in $\mathbb{Z}[x]$.

2.12.3. If k is a field, show that $k[[x]]$ is a local ring. Is $k[x]$ a local ring?

2.12.4. Let k be a field. Show that:
(a) Any $f \in k[[x]] \setminus \{0\}$ can be written as $f = x^k u$ with $k \in \mathbb{N}_0$ and $u \in k[[x]]^\times$.
(b) The ideals in $k[[x]]$ are $\{0\}$ and (x^k), with $k \in \mathbb{N}_0$, thus $k[[x]]$ is a p.i.d.

13. Factorização em anéis de polinómios

Exercícios

2.13.1. Let D be an integral domain and $c \in D$ be an irreducible element. Show that the ideal $(x, c) \subset D[x]$ is not principal. So $D[x]$ is not a p.i.d.

2.13.2. Show that the following rings are not p.i.d.:
(a) $\mathbb{Z}[x]$;
(b) $k[x_1, \ldots, x_n]$, where k is a field and $n \geq 2$.

2.13.3. Let $f = \sum a_i x^i \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}$ be a prime. Let $\bar{f} = \sum \underline{a_i} x^i \in \mathbb{Z}_p[x]$.
(a) Show that, if f is monic and $\bar{f}$ is irreducible in $\mathbb{Z}_p[x]$ for some prime p, then f is irreducible in $\mathbb{Z}[x]$.
(b) Give an example that shows that the previous part is false if f is not a monic polinomial.
(c) Generalize part (a) for polinomials with coefficients in a u.f.d.

2.13.4. (a) Let A be a commutative ring, let $b \in A$ and $c \in A^\times$. Show that there is a unique automorphism of $A[x]$ such that $x \mapsto cx+b$ and whose restriction to A is the identity id_A. Determine its inverse.
(b) Let D be an integral domain and let $\varphi \in \mathrm{Aut}(D[x])$ be such that $\varphi|_D = \mathrm{id}_D$. Show that φ is of the form described in (a).

2.13.5. Let k be a field. Show that x and y are relatively prime (i.e. $\gcd(x, y) = 1$) in $k[x, y]$, but $k[x, y] = (1) \supsetneq (x) + (y)$.

Categorias

1. Definição e exemplos

Exercícios

3.1.1. Let $f : X \to Y$ be an isomorphism in the category $\mathcal{C}$. Show that there is a *unique* mormophism $g : Y \to X$ s.t. $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$.

3.1.2. Show that the Definition 1.14 of isomorphism in the categories $\mathrm{Grp}, \mathrm{Ring}, \mathrm{Vect}_k$ coincide with the definition given before. I.e., show that $f : X \to Y$ is a morphism in the category $\mathcal{C}$ such that there is a morphism $g : Y \to X$ satisfying $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$ iff f is a bijection, where $\mathcal{C}$ is any of the categories $\mathrm{Grp}, \mathrm{Ring}, \mathrm{Vect}_k$.

3.1.3. Show that, in the category $\mathcal{C}_G$ defined in Examplo 1.10, each morphism is an isomorphism, an epimorphism and a monomorphism.

2. Produtos e coprodutos

Exercícios

3.2.1. Let $(S, \{\iota_j\}_{j\in I})$ be a product of the family $\{A_j \mid j \in I\}$ in $\mathcal{C}$. Show that $(S, \{\iota_j\}_{j\in I})$ is a coproduct in $\mathcal{C}^{op}$.

3.2.2. Prove Theorem 2.8.

3.2.3. Show that, in the category Set of sets, any family $\{A_j \mid j \in I\}$ has a coproduct.
Sugestion: Consider

$$\coprod_{j\in I} A_j \coloneqq \big\{(a, j) \in (\cup_{j\in I} A_i) \times I \mid a \in A_j\big\}$$

with the "inclusion" $\iota_j : A_j \to \coprod_{j\in I} A_j$ given by $a \mapsto (a, j)$. The set $\coprod_{j\in I} A_j$ is called *disjoint union* of the sets A_j.

3. Objectos universais

Exercícios

3.3.1. Show that the trivial group $\{\mathbf{1}\}$ is a final and initial object in the category Grp.

3.3.2. Show that the trivial ring $\{\mathbf{0}\}$ is a final object and $\mathbb{Z}$ is an initial object in the category Ring.

3.3.3. Show that an object T is terminal in the category $\mathcal{C}$ iff T is initial in $\mathcal{C}^{op}$.

3.3.4. Given a category $\mathcal{C}$, define a category $\mathcal{D}$ where the initial objects of $\mathcal{D}$ correspond to the coproducts in $\mathcal{C}$.
Sugestion: Example 3.5.

4. Functores e transformações naturais

Exercícios

3.4.1. Show that to give a contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is equivalent to giving a covariant functor $T\colon \mathcal{C}^{op} \to \mathcal{D}^{op}$.

3.4.2. Let G and H be groups and let $f : G \to H$ be a group homomorphism.

(a) Show that $C : \mathrm{Grp} \to \mathrm{Grp}$ defined by $G \mapsto [G, G]$ and $f \mapsto f|_{[G,G]}$ is a functor.

(b) Show that $Q : \mathrm{Grp} \to \mathrm{Grp}$ given by $G \mapsto G/[G, G]$, where $Q(f) : G/[G, G] \to H/[H, H]$ is the group homomorphism induced by f, is a functor.

(c) Show that the canonical projections $\pi_G : G \to G/[G, G]$ define a natural transformation between the identity functor $\mathrm{id} : \mathrm{Grp} \to \mathrm{Grp}$ and the "quotient by the commutator" functor $Q : \mathrm{Grp} \to \mathrm{Grp}$ of the previous part.

3.4.3. Show that there is no functor $\mathrm{Grp} \to \mathrm{Ab}$ which assigns the center $C(G)$ to each group G.

3.4.4. Let $\mathrm{Ob}(\mathcal{C})$ be the set od pairs (A, S), where $A \in \mathrm{Ob}(\mathrm{CRing})$ and $S \subset A$ is a multiplicative set, and let

$$\hom_{\mathcal{C}}((A, S), (B, R)) := \{f \in \hom_{\mathrm{CRing}}(A, B) \mid f(S) \subset R\}\ .$$

(a) Show that $\mathcal{C}$ is a category.

(b) Show that $F(A, S) = S^{-1}A$ defines a functor $F : \mathcal{C} \to \mathrm{CRing}$.

(c) Let $E : \mathcal{C} \to \mathrm{CRing}$ be the forgetful functor defined by $E(A, S) = A$ in the objects of $\mathcal{C}$. Show that the homomorphisms $\varphi_S : A \to S^{-1}A$, $\varphi_S(a) = \frac{a}{\mathbf{1}}$, define a natural transformation between the functors E and F.

4

Módulos

1. Definição e exemplos

2. Homomorfismos e quocientes

Exercícios

4.2.1. In the category Mod_A we have the notions of isomorphism, epimorphism and monomorphism – see Definitions 1.14 and 1.16 in Chapter 3. Given $f \in \hom_A(M,N)$, show that:
(a) f is an isomorphism iff f is bijective;
(b) f is an monomorphism iff f is injective;
Sugestion for ($\Rightarrow$): consider the inclusion $g\colon \ker f \to M$ and the zero aplication for g'.
(c) f is an epimorphism iff f is surjective.
Sugestion for ($\Rightarrow$): considere the canonical projection $h\colon N \to N/\operatorname{im} f$ and the zero aplication for h'.

4.2.2. Let M be a cyclic A-module. Show that there exists a left ideal $I \subset A$ s.t. $M \cong A/I$.

4.2.3. An A-module, $M \neq \{0\}$, is called *simple* if the only submodules are $\{0\}$ and M. Prove the following statements:
(a) Any simple module is cyclic.
(b) Is M is simple, then any endomorphism[1] of M is either zero or an isomorphism.

4.2.4. Let M and N be A-modules. Show that:
(a) $\hom_A(M,N)$ is an abelian group for the sum $f+g$ defined by $(f+g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v})\ \forall\, \mathbf{v} \in M$;
(b) $\mathrm{End}_A(M) \coloneqq \hom_A(M,M)$ is a ring (with identity) with product given by composition of maps;
(c) M is a left module over the ring of endomorphisms[1] $\mathrm{End}_A(M)$, where $f \cdot \mathbf{v} = f(\mathbf{v})$, for $\mathbf{v} \in M$ and $f \in \hom_A(M,M)$.

4.2.5. Let A be a p.i.d, M an A-module and $p \in A$ a prime element. Let

$$pM \coloneqq \{p\mathbf{v} \mid \mathbf{v} \in M\} \qquad \text{and} \qquad M[p] \coloneqq \{\mathbf{v} \in M \mid p\mathbf{v} = 0\}\ .$$

Show that

[1]As in groups and rings, an endomorphism of a module M is an homomorphism $f\colon M \to M$.

(a) $A/(p)$ is a field;
(b) pM and $M[p]$ are sunmodules of M;
(c) M/pM is a vector space over $A/(p)$ with the following product by scalars

$$(a + (p))(\mathbf{v} + pM) = a\mathbf{v} + pM \qquad \forall\, a \in A, \mathbf{v} \in M \ ;$$

(d) $M[p]$ is a vector space over $A/(p)$ with product by scalars given by

$$(a + (p))\mathbf{v} = a\mathbf{v} \qquad \forall\, a \in A, \mathbf{v} \in M \ .$$

3. Produto directo e soma directa

4. Soma directa interna e somandos directos

Exercícios

4.4.1. Let $f\colon M \to M$ be a homomorphism of A-modules such that $f \circ f = f$. Show that $M = \ker f \oplus \operatorname{im} f$.

4.4.2. Show that the short exact sequence of A-modules, $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ splits iff is isomorphic to

$$0 \to M_1 \xrightarrow{\iota_1} M_1 \oplus M_3 \xrightarrow{\pi_2} M_3 \to 0.$$

4.4.3. (Five Lemma.) Consider the following commutative diagram of A-modules

$$\begin{tikzcd} M_1 \arrow[r, "f_1"] \arrow[d, "h_1"'] & M_2 \arrow[r, "f_2"] \arrow[d, "h_2"'] & M_3 \arrow[r, "f_3"] \arrow[d, "h_3"'] & M_4 \arrow[r, "f_4"] \arrow[d, "h_4"'] & M_5 \arrow[d, "h_5"'] \\ N_1 \arrow[r, "g_1"] & N_2 \arrow[r, "g_2"] & N_3 \arrow[r, "g_3"] & N_4 \arrow[r, "g_4"] & N_5 \end{tikzcd}$$

where the lines are exact sequences. Show that:
(a) if h_1 is surjective and h_2, h_4 are injective, then h_3 is injective;
(b) if h_5 is injective and h_2, h_4 are surjective, then h_3 is surjective;
(c) if h_1, h_2, h_4, h_5 are isomorphisms, then h_3 is also an isomorphism.

4.4.4. (a) Given two short exact sequences of A-modules

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow M_3 \xrightarrow{f_3} M_4 \xrightarrow{f_4} M_5 \longrightarrow 0 \ ,$$

show that

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_3 \circ f_2} M_4 \xrightarrow{f_4} M_5 \xrightarrow{f_5} 0$$

is an exact sequence.
(b) Show that any exact sequence of A-modules can be obtained combining short exact sequences as in (a).

4.4.5. The definition of exact sequences in the category of groups is ananlogous to that for modules, that is, in Definição 4.5 we considere groups and group homomorphisms. Given the following short exact sequence of groups

$$\{\mathbf{1}\} \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow \{\mathbf{1}\} \ ,$$

show that as seguintes afirmações são equivalentes:
(a) $G = N' \rtimes H' \cong N \rtimes H$, where $N' = \operatorname{im} \alpha$, for some subgroup $H' < G$ (see Exercise 1.8.5);
(b) There exists a group homomorphism $r\colon H \to G$ such that $\beta \circ r = \mathrm{id}_H$;
(c) There exists a group homomorphism $l\colon G \to N$ such that $l \circ \alpha = \mathrm{id}_N$.
In particular, in the case of one (thus all) of these conditions holds, the group G is not necessarely isomorphic to the direct sum $N \oplus H$, as it happens in the category of A-modules – compare to the Proposition 4.13.

5. Módulos livres

Exercícios

4.5.1. Show that, if $I \neq \{0\}$ is a bilateral ideal of the ring A, then A/I is not free as an A-module.

4.5.2. (a) Let A be a commutative ring, so A is a free A-module and any ideal I is a submodule of A. Show that if the ideal $I \neq \{0\}$ is a free module then I is principal.
Sugestion: Show that any subset of I containing at least two elements is linearly dependent.
(b) Give an example of a commutative ring A and of a principal ideal $I \neq \{0\}$ de A such that I is not a free A-module.

4.5.3. Show that, if $A \neq \{0\}$ is a commutative ring such that any submodule of a free A-module is free, then A is a p.i.d.

4.5.4. Prove Proposition 5.6.

4.5.5. Prove Proposition 5.7.

4.5.6. Let B be a ring and let F be a free B-module with countable basis $\{\mathbf{e}_i \mid i \in \mathbb{N}\}$. Considere the ring $A = \mathrm{End}_B(F)$ – see Exercise 4.2.4.
(a) Define $f_1, f_2 \colon F \to F$ by

$$\begin{cases} f_1(\mathbf{e}_{2i-1}) = \mathbf{e}_i \\ f_1(\mathbf{e}_{2i}) = 0 \end{cases} \qquad \text{and} \qquad \begin{cases} f_2(\mathbf{e}_{2i-1}) = 0 \\ f_2(\mathbf{e}_{2i}) = \mathbf{e}_i \ . \end{cases}$$

Show that $\{f_1, f_2\}$ is a basis for A and conclude that $A \cong A^2$ as A-modules.
(b) Conclude that $A \cong A^n$, for any $n \in \mathbb{N}$.

4.5.7. Let M be an A-module and let X be a set. Then $M \cong F(X)$ iff there exists a map $i \colon X \to M$ s.t. M is a free object generated by (X, i) in Mod_A.

6. Caracterização dos módulos livres; espaços vectoriais

7. Anéis de matrizes

8. Invariância dimensional

Exercícios

4.8.1. (a) Show that $\dim_{\mathbb{R}} \mathbb{C} = 2$ and $\dim_{\mathbb{R}} \mathbb{R} = 1$.
(b) Show that there is no field k such that $\mathbb{R} \subsetneq k \subsetneq \mathbb{C}$.

4.8.2. Let V and W be vector spaces over a division ring D and let $f : V \to W$ be a linear map. Show that $\dim_D V = \dim_D(\ker f) + \dim_D(\operatorname{im} f)$.

4.8.3. (a) Let V and W be finite dimensional vector spaces over a division ring D s.t. $\dim_D V = \dim_D W$ and let $f\colon V \to W$ be a linear map. Show that the following statements are equivalent:
(i) f is an isomorphism;
(ii) f is surjective;
(iii) f is injective.
(b) Give an example that shows that part (a) can be false if V and W have infinite dimension.

4.8.4. Let V be a vector space over a division ring D and let $W \subset V$ be a subspace. Show that:
(a) $\dim_D W \leq \dim_D V$;
(b) $\dim_D W = \dim_D V < \infty \Rightarrow W = V$;
(c) $\dim_D V = \dim_D W + \dim_D(V/W)$.

4.8.5. Considere the real vector space $V = \mathbb{R}[x]$ and let $W = \{f(x) \in V \mid f(0) = 0\}$. Show that W is a subespace of V and that $W \neq V$. Determine a basis for W and another for V, and conclude that $\dim_{\mathbb{R}} W = \dim_{\mathbb{R}} V$. Therefore, part (b) in the previous exercise can be false if the vector spaces have infinite dimensions.

9. Módulos projectivos

Exercícios

4.9.1. Given a commutative ring A, A^n has an $M_n(A)$-module struture, by identifyng vectors in A^n with column matrices, with product by scalars $M_n(A) \times A^n \to A^n$ given by matrix multiplication $(X, \mathbf{v}) \mapsto X\mathbf{v}$.

(a) Show that A^n is not a free $M_n(A)$-module.
Sugestion: Verify that $\{\mathbf{v}\}$ is linearly dependent over $M_n(A)$ for any $\mathbf{v} \in A^n$.

(b) Show that A^n is a projective $M_n(A)$-module.
Sugestion: Identify A^n with a submodule N of $M_n(A)$ and show that N is a direct summand of $M_n(A)$.

4.9.2. Let A be a ring. An element $e \in A$ is *idempotent* if $e^2 = e$. Show that, if $e \in A$ is idempotent, Ae is a projective A-module.

4.9.3. Let $P_i \in \mathrm{Mod}_A$, $i \in I$. Show that $\bigoplus_{i \in I} P_i$ is projective iff P_i is projective $\forall i \in I$.

4.9.4. Show that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module.

4.9.5. Let A be a commutative ring. Given two A-modules, P and M, the set $\hom_A(P, M)$ has an A-module structure defined by

$$(f+g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v}) \qquad \text{and} \qquad (af)(\mathbf{v}) = af(\mathbf{v}) \quad \forall\, \mathbf{v} \in P\ ,$$

with $f, g \in \hom_A(P, M)$ and $a \in A$.

(a) Given an A-module homomorphism, $g : M \to N$, we define

$$g_* : \hom_A(P, M) \to \hom_A(P, N)$$

by $g_*(\varphi) := g \circ \varphi$. Show that the map g_* is a homomorphism of A-modules.

(b) Let

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

be a short exact sequence of A-modules.

(i) If P is any A-module, show that

$$0 \longrightarrow \hom_A(P, L) \xrightarrow{f_*} \hom_A(P, M) \xrightarrow{g_*} \hom_A(P, N)$$

is an exact sequence.

(ii) Show that g_* is surjective iff P is a projective A-module.

10. Módulos injectivos

Exercícios

4.10.1. Prove Proposition 10.4.

4.10.2. Show that the following statements are equivalent:
- (i) any A-module is projective;
- (ii) any short exact sequence of A-modules splits;
- (iii) any A-module is injective.

4.10.3. Show that any vector space over a division ring D is projective and injective.

4.10.4. Prove the following statements:
- (a) no nontrivial finite abelian group is divisible;
- (b) no nontrivial free abelian group[2] is divisible.

4.10.5. Show that the group $\mathbb{Z}(p^\infty)$, where $p \in \mathbb{N}$ is a prime, is divisible.

4.10.6. Let D be a divisible torsion free[3] abelian group.
- (a) Given $n \in \mathbb{Z} \setminus \{0\}$ and $a \in D$, let $b \in D$ be such that $nb = a$. Show that $\frac{1}{n} \cdot a := b$ induces a product by scalars $\mathbb{Q} \times D \to D$ which, together with the sum in D, define a $\mathbb{Q}$-vector space struture in D.
- (b) Conclude that $D \cong \oplus_{i \in I} \mathbb{Q}$.

[2] Recall that an abelian group G is *free* if it is free as a $\mathbb{Z}$-module – see Observation 6.3.

[3] An abelian group G is *torsion free* if the subgroup $\mathrm{Tor}(G) := \{g \in G \mid |g| \text{ is finite}\}$ is the trivial group $\{0\}$ – see Exercise 1.4.12.

11. Produto tensorial

Exercícios

4.11.1. (a) Let G be an abelian group. Show that $G \otimes \mathbb{Z}_m \cong G/mG, \forall\, m > 0$.
(b) Show that $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_d$, where $d = \gcd(m, n)$.
(c) Let G be a torsion abelian group.[4] Show that $G \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.
(d) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

4.11.2. Let M and N A-modules and let $M' \subset M$ and $N' \subset N$ be submodules. Show that

$$M/M' \otimes_A N/N' \cong (M \otimes_A N)/H \ ,$$

where H is the submodule of $M \otimes N$ generated by $\mathbf{v}' \otimes \mathbf{w}$ and $\mathbf{v} \otimes \mathbf{w}'$ for $\mathbf{v}' \in M'$, $\mathbf{v} \in M$, $\mathbf{w}' \in N'$ and $\mathbf{w} \in N$.

4.11.3. Let I and J be ideals in a commutative ring A, let M be an A-module. Show that:
(a) $A/I \otimes_A M \cong M/IM$, as A-modules, where $IM = \langle a\mathbf{v} \mid a \in I, \mathbf{v} \in M\rangle$ is a submodule of M;
(b) $A/I \otimes_A A/J \cong A/(I + J)$, as A-modules.

4.11.4. The inclusion map $\iota : \mathbb{Z}_2 \to \mathbb{Z}_4$ is an abelian group homomorphism, since $\mathbb{Z}_2 < \mathbb{Z}_4$. Show that $\mathrm{id} \otimes \iota \colon \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes \mathbb{Z}_4$ is the null application, however $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \neq 0$ and $\mathbb{Z}_2 \otimes \mathbb{Z}_4 \neq 0$.

4.11.5. Give an example of a commutative ring A and A-modules M and N such that:
(a) $M \otimes_A N \ncong M \otimes_{\mathbb{Z}} N$;
(b) $\exists\, \mathbf{u} \in M \otimes_A N$ such that $\forall\, \mathbf{v} \in M, \forall\, \mathbf{w} \in N \quad \mathbf{u} \neq \mathbf{v} \otimes \mathbf{w}$;
(c) $\exists\, \mathbf{v}, \mathbf{v}' \in M, \mathbf{w}, \mathbf{w}' \in N$ such that $\mathbf{v} \neq \mathbf{v}', \mathbf{w} \neq \mathbf{w}'$ and $\mathbf{v} \otimes \mathbf{w} = \mathbf{v}' \otimes \mathbf{w}'$.

4.11.6. Determine $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$.

4.11.7. Prove Proposition 11.16.

[4] G is a *torsion* abelian group if $G = \mathrm{Tor}(G)$ – see Exercise 1.4.12.

12. Propriedades adicionais do produto tensorial

Exercícios

In the following exercises, A is a commutative ring.

4.12.1. Let N be an A-module and consider the following short exact sequence of A-modules

$$(*) \qquad 0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

Show that

$$0 \longrightarrow N \otimes_A M_1 \xrightarrow{f_1} N \otimes_A M_2 \xrightarrow{f_2} N \otimes_A M_3 \longrightarrow 0$$

is a short exact sequence of A-modules if
(a) the sequence $(*)$ splits; or
(b) N is a free A-module; or
(c) N is a projective A-module.

4.12.2. Let M be an A-module. Define the *dual* of M by

$$M^* := \hom_A(M, A).$$

Show that M^* is an A-module with sum $f+g$ and scalar product[5] af defined respectively by

$$\begin{aligned} (f+g)(\mathbf{v}) &= f(\mathbf{v}) + g(\mathbf{v}) \\ (af)(\mathbf{v}) &= af(\mathbf{v}) \qquad\qquad \forall\, \mathbf{v} \in M\ , \end{aligned}$$

where $f, g \in M^*$ and $a \in A$.

4.12.3. Let M be a free A-module with a basis $\{\mathbf{e}_i\}_{i\in I}$. Let $\mathbf{e}_i^* \in M^*$ (see Exercise 4.12.2) defined by $\mathbf{e}_i^*(\mathbf{e}_j) = \delta_{ij}$, i.e., $\mathbf{e}_i^*(\mathbf{e}_j) = 1$ if $j = i$ and $\mathbf{e}_i^*(\mathbf{e}_j) = 0$ otherwise.
(a) Show that $\{\mathbf{e}_i^*\}_{i\in I}$ is a linearly independent set in M^*.
(b) Show that, if I is finite, then $\{\mathbf{e}_i^*\}_{i\in I}$ is a basis for M^*.
(c) Give an example that shows that $\{\mathbf{e}_i^*\}_{i\in I}$ may not be basis of M^*, if I is an infinite set.

4.12.4. Let M and N be A-modules. Show that $(M \otimes_A N)^* \cong \hom_A(M, N^*)$ (see Exercise 4.12.2).

4.12.5. Let M and N be A-modules.
(a) Let $\varphi \in M^*$ (see Exercício 4.12.2) and $\mathbf{w} \in N$. Show that $\alpha_{\varphi,\mathbf{w}} \colon M \to N$, given by $\mathbf{v} \mapsto \varphi(\mathbf{v})\mathbf{w}$, is an A-linear map.
(b) Show that $\alpha \colon M^* \otimes_A N \to \hom_A(M, N)$ given by $\varphi \otimes \mathbf{w} \mapsto \alpha_{\varphi,\mathbf{w}}$ is an A-linear map.
(c) Show that, if M and N are finitely generated free modules, then the map α in (b) is an isomorphism.
(d) Conclude that $(A^n)^* \otimes_A A^n \cong \mathrm{End}_A(A^n) \cong M_n(A)$. (Compare with Example 11.19.)

[5] If A is not a commutative ring, the dual of a left A-module has a right A-module struture with the product of $f \in M^*$ by a scalar $a \in A$ given by $(fa)(\mathbf{v}) = f(\mathbf{v})a$. Recall that in the commutative case the left and right module notions coincide.

13. Extensão de escalares

Exercícios

4.13.1. (Two changes of scalars.) Let A, B, C be commutative rings and $\alpha\colon A \to B$, $\beta : B \to C$ be ring homomorphisms. If M is an A-module, show that $C \otimes_B (B \otimes_A M) \cong C \otimes_A M$ as C-modules, i.e., $(M_B)_C \cong M_C$, where the B-module struture is induced by α and the C-module structures are induced by β in M_B and by $\beta \circ \alpha$ in M.

4.13.2. (Restriction of scalars.) Let A, B be commutative rings and $\alpha : A \to B$ be a ring homomorphism.
(a) Let N be a B-module. Show that $a \cdot \mathbf{v} := \alpha(a)\mathbf{v}$, together with the sum in N, defines an A-module structure in N. This A-module is denoted by $\operatorname{Res}_A^B N$.
(b) Show that
$$\hom_B(B \otimes_A M, N) \cong \hom_A(M, \operatorname{Res}_A^B N)$$
as B-modules.

4.13.3. (Localization of modules.) Let A be a commutative ring and $S \subset A$ be a multiplicative subset and consider the ring $S^{-1}A$. Given an A-module M define
$$(\mathbf{v}, s) \sim (\mathbf{w}, r) \Leftrightarrow \exists\, x \in S \text{ such that } x(s\mathbf{w} - r\mathbf{v}) = 0,$$
where $(\mathbf{v}, s), (\mathbf{w}, r) \in M \times S$.
(a) Show that $\sim$ is an equivalence relation $M \times S$.
(b) The equivalence class of $(\mathbf{v}, s) \in M \times S$ is denoted by $\frac{\mathbf{v}}{s}$ and the set of equivalence classes is denoted by $S^{-1}M$. Show that $S^{-1}M$ is a $S^{-1}A$-module with the following operations:
$$\frac{\mathbf{v}}{s} + \frac{\mathbf{w}}{r} := \frac{r\mathbf{v} + s\mathbf{w}}{sr} \qquad \text{and} \qquad \frac{a}{t} \cdot \frac{\mathbf{v}}{s} := \frac{a\mathbf{v}}{ts}\ ,$$
where $\frac{\mathbf{v}}{s}, \frac{\mathbf{w}}{r} \in S^{-1}M$ and $\frac{a}{t} \in S^{-1}A$. (In particular, don't forget to show that the operations are well-defined.)
(c) Since $\varphi_S\colon A \to S^{-1}A$, $a \mapsto \frac{a}{1}$ is a ring homomorphism, $S^{-1}M$ has a natural A-module structure. Show that
$$\psi_S\colon M \to S^{-1}M\ , \quad \mathbf{v} \mapsto \frac{\mathbf{v}}{1}$$
is an A-module homomorphism such that $\varphi_S(a)\psi_S(\mathbf{v}) = \psi_S(a\mathbf{v})$. This homomorphism ψ_S is the canonical homomorphism of the localization $S^{-1}M$.

4.13.4. Let A be a commutative ring, $S \subset A$ a multiplicative set and M an A-module. Consider the localization $S^{-1}A$ of A and $S^{-1}M$ of M, and the canoninal homomorphisms $\varphi_S\colon A \to S^{-1}A$ and $\psi_S\colon M \to S^{-1}M$ – see Exercise 4.13.3.
(a) Show that
$$\alpha\colon S^{-1}A \otimes_A M \to S^{-1}M\ , \quad \frac{a}{s} \otimes \mathbf{v} \mapsto \frac{a\mathbf{v}}{s}$$
is well-defined and is an isomorphism of $S^{-1}A$-modules.
(b) Let
$$\begin{aligned}\phi_{S^{-1}A,M}\colon M &\to S^{-1}A \otimes_A M\\ \mathbf{v} &\mapsto \varphi_S(1) \otimes \mathbf{v} = \frac{1}{1} \otimes \mathbf{v}\ ,\end{aligned}$$
be the homomorphism associated to the change of scalars induced by φ_S. Show that $\alpha \circ \phi_{S^{-1}A,M} = \psi_S$.

14. Módulos sobre domínios integrais

Exercícios

4.14.1. Let k be a field, $V \in \mathrm{Vect}_k$ and $T \in \hom_k(V, V)$. Consider the $k[x]$-module structure in V described in Example 14.2.5, i.e., with the product by scalars in $k[x]$ induced by $x \cdot \mathbf{v} := T(\mathbf{v})$, for $\mathbf{v} \in V$. If $\dim_k V = n$ is finite, show that $\mathrm{Tor}_{k[x]} V = V$.
Sugestion: Consider the vectors $\mathbf{v}, T(\mathbf{v}), \dots, T^n(\mathbf{v})$.

4.14.2. Let M_i D-modules, $i \in I$.
(a) Show that $\mathrm{Tor}\left(\prod_{i\in I} M_i\right) \subset \prod_{i\in I} \mathrm{Tor}(M_i)$.
(b) Is it always true that $\mathrm{Tor}\left(\prod_{i\in I} M_i\right) = \prod_{i\in I} \mathrm{Tor}(M_i)$?

4.14.3. Considere the following short exact sequence in Mod_D

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0 .$$

(a) Show that

$$0 \longrightarrow \mathrm{Tor}(M) \xrightarrow{f|_{\mathrm{Tor}\, M}} \mathrm{Tor}\, N \xrightarrow{g|_{\mathrm{Tor}\, N}} \mathrm{Tor}\, P$$

is an exact sequence.
(b) Give an example of a surjective homomorphism $g : M \to P$ such that the restrictions $g|_{\mathrm{Tor}\, N} : \mathrm{Tor}\, N \to \mathrm{Tor}\, P$ is not surjective.

4.14.4. Prove Proposition 14.9(a).

4.14.5. Let D be an integral domain and let M be a free D-module. Show that M is torsion free. By giving a counter-example, show that the converse is false.

4.14.6. Let D be an integral domain with fraction field $K = \mathrm{Frac}(D)$ and let M be a D-module. Recall that $\mathrm{Frac}(D) = S^{-1}D$ with $S = D \setminus \{0\}$, and consider the K-vector space $N = S^{-1}M$ – see Exercise 4.13.3.
(a) Let $\psi_S : M \to S^{-1}M$ be the canonical homomorphism given by $\mathbf{v} \mapsto \frac{\mathbf{v}}{1}$. Show that $\ker \psi_S = \mathrm{Tor}\, M$.
(b) Conclude that $\ker \phi = \mathrm{Tor}\, M$, where $\phi = \phi_{K,M} : M \to K \otimes_D M; \mathbf{v} \to 1 \otimes \mathbf{v}$.
Sugestion: Exercise 4.13.4.

15. Módulos sobre um *d.i.p.*

Exercícios

4.15.1. Consider the following elementary operations

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \xrightarrow{(iii)} \begin{bmatrix} a & b \\ 0 & b \end{bmatrix} \xrightarrow{(iv)+(iii)} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

where (iv) is applied to the columns. Write c, d in terms of a, b and conclude that $c \mid d$. Repeat the exercise for 3×3 diagonal matrices.

4.15.2. Determine the invariant factors of the following matrices with entries in $\mathbb{Z}$:

$$A = \begin{bmatrix} 12 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 \\ 0 & 0 & 150 & 0 \\ 0 & 0 & 0 & 18 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 4 & 2 & -2 \\ 2 & -10 & 6 \end{bmatrix}$$

4.15.3. Prove Theorem 15.11 in the general case, i.e., when N is not necessarily finitely generated.

16. Classifificação de módulos finitamente gerados sobre *d.i.p.*

Exercícios

4.16.1. (a) Let D be a p.i.d and M be a finitely generated torsion A-module. Show that $I = \{d \in D \mid dM = 0\}$ is a non zero ideal in D. An element $a \in I$ is called q *minimal annihilator* of M.

(b) Give an example of a finite abelian group M with minimal annihilator $m \in \mathbb{Z}$ and a cyclic subgroup N with order $n \in \mathbb{N}$ satisfying $n \mid m$ and $n \neq \pm 1$, $n \neq \pm m$ such that N is not a direct summand of M.

4.16.2. Let D be a p.i.d. and let M be a cyclic D-module of order[6] $a \in D$. Show that:

(a) Given $b \in D$ such that a and b relatively prime, then $bM = M$ and $M[b] = 0$. (See Exercise 4.2.5 for the definitions of bM and $M[b]$.)

(b) If $b \mid a$ in D, i.e., if $bc = a$ for some $c \in D$, then $bM \cong D/(c)$ and $M[b] \cong D/(b)$.

4.16.3. Let M be the module over $\mathbb{Z}[i]$ generated by elements x, y whose relations are determined by $(1+i)x + (2-i)y = 0$ and $3x + 5y = 0$. Write M as a direct sum of cyclic modules.

4.16.4. Let G be the abelian group generated by elements x, y, z whose relations are generated by

$$\begin{aligned} 6x + 4y &= 0 \\ 4x + 4y + 12z &= 0 \\ 8x + 8y + 36z &= 0\ . \end{aligned}$$

Determine the invariant factors of G.

4.16.5. Let D be a p.i.d. and let M be a cyclic D-module of order[6] $a \in D$. Show that:

(a) The order of any cyclic submodule of M divides a.

(b) For any ideal $(b) \supset (a)$, M contains precisely one cyclic submodule of order b.

4.16.6. Let D be p.i.d. and let M and N be D-modules of orders[6] $a \neq 0$ and $b \neq 0$, respectively, such that a and b are not relatively prime. Show that $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are the invariant factors of $M \oplus N$.

[6] The cyclic D-module $M = \langle \mathbf{v} \rangle$ has *order* $a \in D$ if $\operatorname{ann}(\mathbf{v}) = (a) \subset D$.

17. Decomposição em factores cíclicos primários

18. Relação entre divisores invariantes e elementares

Exercícios

4.18.1. Let $G = \mathbb{Z}^3/\operatorname{im} f$, where $f\colon \mathbb{Z}^2 \to \mathbb{Z}^3$ is given by $f(x, y) = (2x + y + z, 3x, x + y)$. Determine the decomposition of G into primary cyclic factors.

4.18.2. How many subgroups of order p^2 does the abelian group $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ contain?

4.18.3. (a) What are the elementary divisors of the abelian group $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{15}$? What are the invariant factors of that group?
(b) Repeat part (a) for $\mathbb{Z}_{42} \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_{200} \oplus \mathbb{Z}_{1000}$.

4.18.4. Up to isomorphism, find all abelian groups of orders 32 and 72.

4.18.5. Up to isomorphism, find all abelian groups of oeder n for $n \leq 20$.

4.18.6. Let $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Show that the invariant factors of the abelian group G are $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$, if $\gcd(m, n) > 1$, and mn, if $\gcd(m, n) = 1$.

4.18.7. Let G be a finite abelian group and $H < G$. Show that G has a subgrupo isomorphic to G/H.

19. Unicidade da decomposição em factores cíclicos primários

Exercícios

4.19.1. Prove Proposition 19.3.

4.19.2. Let $p, q \in D$ be prime elements. Recall the definitions of bM and $M[b]$ in Exercise 4.2.5 and show that
(a) $M(p) = \bigcup_{n\in\mathbb{N}} M[p^n]$;
(b) $D(p) = \{0\}$;
(c) $\big(D/(q^m)\big)(p) \neq \{0\}$ if and only if $q \sim p$, where $m \in \mathbb{N}$;
(d) $p^l\big(D/(p^m)\big) \cong D/(p^{l-m})$, for $l < m$, and $p^l\big(D/(p^m)\big) = \{0\}$, for $l \geq m$.
Sugestion: Use the results in Exercise 4.16.2.

20. Formas canónicas racionais

21. Forma canónica de Jordan

Exercícios

4.21.1. Prove Lemma 20.1.

4.21.2. Let k be a field, V a k-vector space and $T \in \mathrm{End}_k(V)$. Consider the usal $k[x]$-module structure in V induced by $x\mathbf{v} := T(\mathbf{v})$. Show that

$$k[x] \otimes_{k[x]} V \cong k[x] \otimes_k V / \langle \{x \otimes \mathbf{v} - 1 \otimes T\mathbf{v} \mid \mathbf{v} \in V\} \rangle$$

as $k[x]$-modules.

4.21.3. Find the Jordan canonical form of the following matrices in $M_4(\mathbb{C})$:

$$A = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 4 & 1 & 1 & -1 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 \\ 1 & 1 & 2 & 2 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 4 & -1 & 0 & -1 \\ 0 & 3 & 0 & 0 \\ -1 & 1 & 3 & 2 \\ 1 & -1 & 0 & 2 \end{bmatrix}.$$

4.21.4. Let $A \in M_n(\mathbb{R})$. Show that A is conjugate to a matrix in the form

$$\begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix},$$

where each B_j is either a Jordan block for an eigen value $\lambda_j \in \mathbb{R}$, or has the form

$$B_j = \begin{bmatrix} A_j & I & & \\ & A_j & \ddots & \\ & & \ddots & I \\ & & & A_j \end{bmatrix},$$

with $A_j = \begin{bmatrix} a_j & -b_j \\ b_j & a_j \end{bmatrix}$, $a_j, b_j \in \mathbb{R}$ and $b_j \neq 0$, and $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Sugestion: Consider the inclusion $M_n(\mathbb{R}) \subset M_n(\mathbb{C})$, and find a basis for $\mathbb{R}^n$ in terms of a basis for $\mathbb{C}^n$ which transforms A in its Jordan canonical form $J \in M_n(\mathbb{C})$. To do that, consider separate cases for eigen values in $\mathbb{R}$ and in $\mathbb{C} \setminus \mathbb{R}$.

22. Aplicações das formas canónicas e dos factores invariantes e elementares

Exercícios

4.22.1. Find the conjugation classes in the groups
(a) $GL_3(\mathbb{C})$;
(b) $GL_3(\mathbb{Z}_2)$;
(c) $GL_4(\mathbb{R})$.
In (b), write explicitly a representative in each class.

4.22.2. Decide if the following pairs of matrices are conjugate in the given groups:

(a) $\begin{bmatrix} 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ in $GL_4(\mathbb{Q})$;

(b) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ in $GL_3(\mathbb{Z}_5)$;

(c) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ in $GL_4(\mathbb{Z}_2)$.

4.22.3. Consider the k-vector space (where k is a field)

$$V = \frac{k[x]}{(f(x))} \otimes_k \frac{k[x]}{(g(x))}$$

with the $k[x]$-module structure induced by $T \in \mathrm{End}_k(V)$ defined by

$$T\big(\underline{a(x)} \otimes \underline{b(x)}\big) = \underline{xa(x)} \otimes \underline{xb(x)} \ ,$$

for $a(x), b(x) \in k[x]$. Find the invariant and the primary cyclic decompositions of V as $k[x]$-modules when
(a) $f(x) = g(x) = x^2 - 3$ and $k = \mathbb{Q}$;
(b) $f(x) = (x-3)^2$, $g(x) = x^2 - 1$ and $k = \mathbb{C}$.

Teoria de representação de grupos

1. Representações

Exercícios

6.1.1. (a) Determine the 1-dimensional real (over $\mathbb{R}$) representations of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(b) Determine the 1-dimensional real representations of the group D_4.
Sugestion: Compute $[D_4, D_4]$ and verify that $D_4/[D_4, D_4] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

6.1.2. Proof Lemmas 1.15 and 1.17.

6.1.3. Let G be a finite group, and let $\bar{g} = \sum_{g \in G} g \in k(G)$. Let $W = \langle \bar{g} \rangle = \{a\bar{g} \in k(G) \mid a \in k\}$. Show that W is a subrepresentaion of the regular representation $k(G)$ which is trivial.

6.1.4. (a) Let G be a finite abelian group and let k be an algebraically closed field. Show that any irreducible representation of G has dimension 1.
(b) Let G be a cyclic group of order 4 with generator a. Considere the following real representation V with action $\rho : G \to GL_2(\mathbb{R})$ defined by

$$\rho(a) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} .$$

Show that V is irreducible over $\mathbb{R}$.

6.1.5. Let $G = \{\mathbf{1}_G, a\}$ a cyclic group of order 2 and consider the regular representation $\mathbb{R}(G)$. Let $V_1 = \{x\mathbf{1}_G + xa \in \mathbb{R}(G) \mid x \in \mathbb{R}\}$ and $V_2 = \{x\mathbf{1}_G - xa \in \mathbb{R}(G) \mid x \in \mathbb{R}\}$.
(a) Show that V_1 and V_2 are subrepresentations of the regular representation $\mathbb{R}(G)$. What are the dimensions?
(b) Show that V_1 is a trivial representation and V_2 is equivalent to the sign resentation.
(c) Show that $\mathbb{R}(G) = V_1 \oplus V_2$.

6.1.6. Let $G = \{\mathbf{1}_G, a\}$ be the cyclic group of order 2 and consider the regular representation $\mathbb{Z}_2(G)$. Let $V = \{x\mathbf{1}_G + xa \in \mathbb{Z}_2(G) \mid x \in \mathbb{Z}_2\}$. Show that V is a subrepresentation of the regular representation $\mathbb{Z}_2(G)$ which doesn't have a complement. (Compare with the previous exercise.)

6.1.7. Let $V \neq \{0\}$ be an irreducible representation of G. Show that there exists a maximal left ideal I of the ring $k(G)$ such that $V \cong k(G)/I$ as $k(G)$-modules.
Sugestion: Apply Schur's Lemma 1.23.

2. Caracteres

Exercícios

6.2.1. Let V and W be two representations of G and "homomorphism" representation $U = \hom_k(V, W)$ in Example 2.6. Show that $U^G = \hom_G(V, W)$.

6.2.2. Show that a complex representation V is irreducible if and only if $\langle \chi_V, \chi_V \rangle = 1$.

6.2.3. Determine if the representations in Examples 1.7 and 1.8 are irreducible over $\mathbb{C}$. If not, determine their decomposition as a direct sum of irreducible representations.

6.2.4. Determine the complex irreducible representations of the following groups:
(a) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} < \mathbb{H}^\times$;
(b) D_4;
(c) D_5.

6.2.5. Determine the character table of A_4 and S_4.

6.2.6. (a) If V is a 1-dimensional representation and W is an irreducible representations, show that $V \otimes W$ is irreducible.
(b) Give an example of a group G and two irreducible representations V, W of G such that $V \otimes W$ is not irreducible.

6.2.7. Let V be a finite dimensional representation. Show that V is irreducible if and only if V^* is irreducible.