T1 – Trabalho semanal 1 de Álgebra Comutativa – Semestre 2021-2

Semana: 31 de janeiro - 4 de fevereiro, 2022.
Prazo de entrega: 16 de fevereiro, 2022.

Cada um dos 5 itens vale 2 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Mostre que os ideais maximais de $\mathbb{Z}[X]$ são todos da forma $(p, P(X))$ com p um número inteiro primo (positivo) e $P(X)$ um polinômio de $\mathbb{Z}[X]$ cuja redução módulo p é irredutível em $\mathbb{F}_p[X]$. Aqui $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

2. Mostre que $\mathbb{R}[X]/(X^2 + X + 1) \cong \mathbb{C}$ e que $\mathbb{R}[X]/(X^2 + X) \cong \mathbb{R} \times \mathbb{R}$.

3. Seja R um anel finito. Mostre que os ideais primos de R são maximais.

4. Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideais primos de um anel R e seja I um ideal de R contido na união $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$. Mostre que I está contido em um dos $\mathfrak{p}_i$.

5. Seja I um ideal do anel R e seja S um subconjunto de R. Seja

$$(I : S) := \{r \in R \ : \ rs \in I \ \forall s \in S\}.$$

   Observe que $(I : S) \trianglelefteq R$ e que $(I : S)$ é o maior ideal J de R tal que $JS \subseteq I$. Em particular $I \subseteq (I : S)$.

   Por exemplo $(I : S) = R$ se $S \subseteq I$ e $(I : S) = I$ se $1 \in S$.

   Sejam I, J dois ideais de R. Mostre que $(I : J) = I$ e $(J : I) = J$ nos dois casos seguintes.

   - $I + J = R$.
   - I, J são primos com $I \not\subseteq J$ e $J \not\subseteq I$.

T1 – Trabalho semanal 1 de Álgebra Comutativa - Resolução

1. Mostre que os ideais maximais de $\mathbb{Z}[X]$ são todos da forma $(p, P(X))$ com p um número inteiro primo (positivo) e $P(X)$ um polinômio de $\mathbb{Z}[X]$ cuja redução módulo p é irredutível em $\mathbb{F}_p[X]$. Aqui $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

   Seja I um ideal maximal de $\mathbb{Z}[X]$. Temos $I \neq \{0\}$ pois $\mathbb{Z}[X]$ não é um corpo.

   Observe que $I \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$, sendo a preimagem de I por meio da inclusão $\mathbb{Z} \to \mathbb{Z}[X]$. Segue que $I \cap \mathbb{Z} = \{0\}$ ou $I \cap \mathbb{Z} = p\mathbb{Z}$ para algum número primo p.

   Suponha que $I \cap \mathbb{Z} = \{0\}$. Considere o ideal J gerado por I em $\mathbb{Q}[X]$. Como $\mathbb{Q}[X]$ é um PID, existe $f(X) \in \mathbb{Q}[X]$ tal que $J = (f(X))$, e podemos obviamente supor que $f(X)$ tenha coeficientes inteiros e que o MCD dos coeficientes seja 1. Observe que todo elemento de J é do tipo $f(X)h(X)$ com $h(X) \in \mathbb{Q}[X]$ e também do tipo $a \cdot k(X)$ com $a \in \mathbb{Q}$ e $k(X) \in I$. Observe que $1 \notin J$ pois caso contrário existiriam $k(X) \in I$, $a \in \mathbb{Q}$ tais que $a \cdot k(X) = 1$, e escrevendo $a = r/s$ com r, s inteiros e $s \neq 0$ obteriamos $s = r \cdot k(X) \in I \cap \mathbb{Z}$, uma contradição. Logo $f(X)$ tem grau positivo. Mostraremos que $I = (f(X))$. Como $f(X) \in J$ existem $a = r/s \in \mathbb{Q}$ (com $r, s \neq 0$ inteiros e r, s coprimos), $k(X) \in I$ tais que $f(X) = a \cdot k(X)$, ou seja $sf(X) = rk(X)$. Seja d o MDC dos coeficientes de $k(X)$, temos então $s = rd$ pelo lema de Gauss, logo $r = \pm 1$ pois r, s são coprimos, segue que $s \cdot f(X) \in I$. Como I é um ideal maximal, é um ideal primo, e sendo $0 \neq s \in \mathbb{Z}$ e $I \cap \mathbb{Z} = \{0\}$ deduzimos que $f(X) \in I$. Isso mostra que $(f(X)) \subseteq I$. Como todo elemento de I é do tipo $f(X)h(X)$ com $h(X) \in \mathbb{Q}[X]$ e tem coeficientes inteiros, pelo lema de Gauss $h(X)$ tem coeficientes inteiros. Isso mostra que $I \subseteq (f(X))$.

   Segue que I é principal gerado por um polinômio $f(X)$. Seja $R = \mathbb{Z}[X]/I$. Como $I \cap \mathbb{Z} = \{0\}$, o homomorfismo canônico $\mathbb{Z} \to R$ é injetivo, logo R é um anel infinito. Seja $a \in \mathbb{Z}$ tal que $f(a) \neq \pm 1$ e seja p um divisor primo de $f(a)$. Podemos definir um homomorfismo sobrejetivo de aneis da forma seguinte, usando o fato que $f(a) \equiv 0 \mod p$.

   $$\psi : R \to \mathbb{Z}/p\mathbb{Z}, \qquad \psi(P(X) + I) := P(a) \mod p$$

   Como R é infinito, $\ker(\psi) \neq \{0\}$. Se $\psi(1) = 0$ então existem polinômios $h(X), k(X) \in \mathbb{Z}[X]$ tais que $p \cdot h(X) + k(X)f(X) = 1$, e substituindo $X = a$ obtemos uma contradição pois p divide $f(a)$. Deduzimos que $1 \notin \ker(\psi)$, logo $\ker(\psi) \neq \{0\}, R$, uma contradição, pois R é um corpo.

   Deduzimos que $I \cap \mathbb{Z} = p\mathbb{Z}$ para algum número primo p. Considere $I/p\mathbb{Z}[X]$, se trata de um ideal de $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong \mathbb{F}_p[X]$. Como $\mathbb{F}_p[X]$ é um PID, existe $f(X) \in \mathbb{Z}[X]$ tal que $I/p\mathbb{Z}[X]$ corresponde a $(\overline{f(X)})$ em $\mathbb{F}_p[X]$, onde $\overline{f(X)} = f(X) + p\mathbb{Z}[X]$, assim $(p, f(X)) = I$.

2. Mostre que $\mathbb{R}[X]/(X^2+X+1) \cong \mathbb{C}$ e que $\mathbb{R}[X]/(X^2+X) \cong \mathbb{R}\times\mathbb{R}$.

   Considere $f : \mathbb{R}[X] \to \mathbb{C}$, $f(P(X)) := P((-1+i\sqrt{3})/2)$. É um homomorfismo sobrejetivo de aneis cujo núcleo é (X^2+X+1), e o resultado segue do teorema de isomorfismo. O segundo isomorfismo pode ser mostrado usando o teorema chinês dos restos: os ideais $I = (X)$, $J = (X+1)$ de $\mathbb{R}[X]$ são coprimos e $IJ = (X(X+1)) = (X^2+X)$, logo

$$\mathbb{R}[X]/(X^2+X) \cong \mathbb{R}[X]/(X) \times \mathbb{R}[X]/(X+1) \cong \mathbb{R}\times\mathbb{R}.$$

3. Seja R um anel finito. Mostre que os ideais primos de R são maximais.

   Seja I um ideal primo de R. Então R/I é um domínio finito. Estamos então reduzidos a mostrar que um domínio finito é um corpo. Seja então R um domínio finito. Se $0 \neq a \in R$ então a função $f : R \to R$ dada por $f(r) := ar$ é injetiva, pois se $ar_1 = ar_2$ então $a(r_1 - r_2) = 0$ e isso implica que $r_1 = r_2$ sendo R um domínio e $a \neq 0$. Pelo princípio da casa dos pombos, como R é finito e $f : R \to R$ é injetiva, f é sobrejetiva, logo existe $r \in R$ tal que $f(r) = 1$, ou seja $ar = 1$. Isso mostra que a é inversível. Segue que todo elemento não nulo de R é inversível, ou seja R é um corpo.

4. Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideais primos de um anel R e seja I um ideal de R contido na união $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$. Mostre que I está contido em um dos $\mathfrak{p}_i$.

   Por indução sobre n, observando que o caso $n = 1$ é trivial. Suponha o resultado verdadeiro para n e sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n+1}$ ideais primos de R tais que $I \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_{n+1}$. Se I está contido na união de n desses ideais primos então a conclusão segue por indução, logo podemos supor que I não está contido em $\bigcup_{j\neq i} \mathfrak{p}_j$ para todo $i = 1, \ldots, n+1$, logo podemos encontrar um $x_i \in I$ tal que $x_i \notin \bigcup_{j\neq i} \mathfrak{p}_j$, para todo $i = 1, \ldots, n+1$. Segue que $x_i \in \mathfrak{p}_i$ para todo $i = 1, \ldots, n+1$. Considere o elemento

$$x := x_1 \cdots x_n + x_{n+1} \in I.$$

   Como $I \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_{n+1}$, existe $i \in \{1, \ldots, n+1\}$ tal que $x \in \mathfrak{p}_i$. Se $i \leq n$ então $x_{n+1} \in \mathfrak{p}_i$, contradição, e se $i = n+1$ então $x_1 \cdots x_n \in \mathfrak{p}_{n+1}$, logo existe $j \in \{1, \ldots, n\}$ tal que $x_j \in \mathfrak{p}_{n+1}$, uma contradição.

5. Seja I um ideal do anel R e seja S um subconjunto de R. Seja

$$(I : S) := \{r \in R \ : \ rs \in I \ \forall s \in S\}.$$

   Observe que $(I : S) \trianglelefteq R$ e que $(I : S)$ é o maior ideal J de R tal que $JS \subseteq I$. Em particular $I \subseteq (I : S)$.

   Por exemplo $(I : S) = R$ se $S \subseteq I$ e $(I : S) = I$ se $1 \in S$.

   Sejam I, J dois ideais de R. Mostre que $(I : J) = I$ e $(J : I) = J$ nos dois casos seguintes.

- $I + J = R$. Neste caso existem $i \in I$, $j \in J$ tais que $i + j = 1$. Se $x \in (I : J)$ então $x = x(i + j) = xi + xj$ pertence a I porque $xi \in I$ e $xj \in I$ sendo $x \in (I : J)$. A demonstração de $(J : I) = J$ é analoga.
- I, J são primos com $I \not\subseteq J$ e $J \not\subseteq I$. Se $x \in (I : J)$ então seja $j \in J - I$, temos que $xj \in I$ pois $x \in (I : J)$, e como I é primo e $j \notin I$, segue que $x \in I$. A demonstração de $(J : I) = J$ é analoga.

T2 – Trabalho semanal 2 de Álgebra Comutativa – Semestre 2021-2

Semana: 7 - 11 de fevereiro, 2022.
Prazo de entrega: 23 de fevereiro, 2022.

Cada um dos 4 itens vale 2.5 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Seja R um anel. Considere o diagrama seguinte de R-módulos e homomorfismos R-lineares.

$$\begin{array}{ccccccccc} A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \xrightarrow{\gamma'} & D' & \xrightarrow{\delta'} & E' \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle e} \\ A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \xrightarrow{\gamma} & D & \xrightarrow{\delta} & E \end{array}$$

   Suponha que

   - O diagrama é comutativo, ou seja

$$b \circ \alpha' = \alpha \circ a, \qquad c \circ \beta' = \beta \circ b, \qquad d \circ \gamma' = \gamma \circ c \qquad e \circ \delta' = \delta \circ d.$$

   - As duas linhas são exatas, ou seja

$$\ker(\beta') = \mathrm{Im}(\alpha'), \qquad \ker(\gamma') = \mathrm{Im}(\beta'), \qquad \ker(\delta') = \mathrm{Im}(\gamma'),$$

$$\ker(\beta) = \mathrm{Im}(\alpha), \qquad \ker(\gamma) = \mathrm{Im}(\beta), \qquad \ker(\delta) = \mathrm{Im}(\gamma).$$

   Suponha que a, b, d, e são isomorfismos. Mostre que c é um isomorfismo.

2. Sejam R um anel, M um R-módulo finitamente gerado e $\varphi : M \to R^n$ um homomorfismo R-linear sobrejetivo.

   (a) Mostre que existe um homomorfismo R-linear $\psi : R^n \to M$ tal que $\varphi \circ \psi = \mathrm{Id}_{R^n}$.

   (b) Mostre que $M \cong \ker(\varphi) \oplus \mathrm{Im}(\psi)$ (isomorfismo R-linear). [Dica: mostre que $\ker(\varphi) \cap \mathrm{Im}(\psi) = \{0\}$ e que $\ker(\varphi) + \mathrm{Im}(\psi) = M$.]

   (c) Mostre que $\ker(\varphi)$ é finitamente gerado.

3. Seja $n \geq 1$ um inteiro e considere o $\mathbb{Z}$-módulo livre $M := \mathbb{Z}^n$. Sejam $b_i = (a_{i1}, \ldots, a_{in})$, $i = 1, \ldots, n$, elementos de M, e seja $E := \{b_1, \ldots, b_n\}$. Seja A a matriz quadrada $(a_{i,j})_{i,j=1,\ldots,n}$. Mostre que

   - E é linearmente independente (sobre $\mathbb{Z}$) se e somente se $\det(A) \neq 0$.
   - E é uma base de M se e somente se $\det(A) = \pm 1$.

4. Sejam R um anel, M um R-módulo e N um R-submódulo de M. Mostre que se os R-módulos N e M/N são finitamente gerados então M é finitamente gerado. Vale o vice-versa?

T2 – Trabalho semanal 2 de Álgebra Comutativa - Resolução

1. Seja R um anel. Considere o diagrama seguinte de R-módulos e homomorfismos R-lineares.

$$\begin{array}{ccccccccc} A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \xrightarrow{\gamma'} & D' & \xrightarrow{\delta'} & E' \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle e} \\ A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \xrightarrow{\gamma} & D & \xrightarrow{\delta} & E \end{array}$$

Suponha que

- O diagrama é comutativo, ou seja

$$b \circ \alpha' = \alpha \circ a, \quad c \circ \beta' = \beta \circ b, \quad d \circ \gamma' = \gamma \circ c \quad e \circ \delta' = \delta \circ d.$$

- As duas linhas são exatas, ou seja

$$\ker(\beta') = \mathrm{Im}(\alpha'), \qquad \ker(\gamma') = \mathrm{Im}(\beta'), \qquad \ker(\delta') = \mathrm{Im}(\gamma'),$$

$$\ker(\beta) = \mathrm{Im}(\alpha), \qquad \ker(\gamma) = \mathrm{Im}(\beta), \qquad \ker(\delta) = \mathrm{Im}(\gamma).$$

Suponha que a, b, d, e são isomorfismos. Mostre que c é um isomorfismo.

Suponha que $x \in C'$ é tal que $c(x) = 0$. Então $d(\gamma'(x)) = \gamma(c(x)) = \gamma(0) = 0$, logo $\gamma'(x) \in \ker(d) = \{0\}$ e isso implica que $\gamma'(x) = 0$, logo $x \in \ker(\gamma') = \mathrm{Im}(\beta')$. Seja $y \in B'$ tal que $x = \beta'(y)$. Segue que $0 = c(x) = c(\beta'(y)) = \beta(b(y))$ logo $b(y) \in \ker(\beta) = \mathrm{Im}(\alpha)$, logo existe $z \in A$ tal que $b(y) = \alpha(z)$ e como a é sobrejetiva existe $t \in A'$ tal que $z = a(t)$. Segue que $b(y) = \alpha(z) = \alpha(a(t)) = b(\alpha'(t))$ logo $y = \alpha'(t)$ pois b é injetiva. Segue que $x = \beta'(y) = \beta'(\alpha'(t)) = 0$.

Suponha que $x \in C$. Como d é sobrejetiva existe $y \in D'$ tal que $\gamma(x) = d(y)$, logo $0 = \delta(\gamma(x)) = \delta(d(y)) = e(\delta'(y))$, logo $\delta'(y) = 0$ sendo e injetiva, logo $y \in \ker(\delta') = \mathrm{Im}(\gamma')$, segue que existe $z \in C'$ tal que $y = \gamma'(z)$, logo $\gamma(x) = d(y) = d(\gamma'(z)) = \gamma(c(z))$ e isso implica que $\gamma(x - c(z)) = 0$, logo $x - c(z) \in \ker(\gamma)$. Como $\ker(\gamma) = \mathrm{Im}(\beta)$, existe $t \in B$ tal que $x - c(z) = \beta(t)$. Como b é sobrejetiva existe $s \in B'$ tal que $t = b(s)$, logo $\beta(t) = \beta(b(s)) = c(\beta'(s))$, segue que $x = c(z) + \beta(t) = c(z) + c(\beta'(s)) = c(z + \beta'(s))$.

2. Sejam R um anel, M um R-módulo finitamente gerado e $\varphi : M \to R^n$ um homomorfismo R-linear sobrejetivo.

   (a) Mostre que existe um homomorfismo R-linear $\psi : R^n \to M$ tal que $\varphi \circ \psi = \mathrm{Id}_{R^n}$.

   Seja e_i o elemento de R^n que tem 1 na componente i e 0 nas outras componentes: $e_i = (0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)$. É um elemento de R^n, para todo $i = 1, \ldots, n$. Como φ é sobrejetivo, existem $m_i \in M$ tais

que $\varphi(m_i) = e_i$ para $i = 1, \ldots, n$. Pela propriedade universal do R-módulo livre sobre $\{m_1, \ldots, m_n\}$, existe um homomorfismo R-linear $\psi : R^n \to M$ tal que $\psi(e_i) = m_i$ para todo $i = 1, \ldots, n$, logo $\varphi \circ \psi$ fixa e_i para todo $i = 1, \ldots, n$, logo é a identidade de R^n.

(b) Mostre que $M \cong \ker(\varphi) \oplus \mathrm{Im}(\psi)$ (isomorfismo R-linear). [Dica: mostre que $\ker(\varphi) \cap \mathrm{Im}(\psi) = \{0\}$ e que $\ker(\varphi) + \mathrm{Im}(\psi) = M$.]

Seja $m \in \ker(\varphi) \cap \mathrm{Im}(\psi)$, então $m = \psi(t)$ para um oportuno $t \in A^n$ e $\varphi(m) = 0$. Segue que $t = \varphi(\psi(t)) = \varphi(m) = 0$. Isso mostra que $\ker(\varphi) \cap \mathrm{Im}(\psi) = \{0\}$.

Seja $m \in M$. Então $\varphi(m - \psi(\varphi(m))) = \varphi(m) - \varphi(\psi(\varphi(m))) = \varphi(m) - \varphi(m) = 0$, logo $m - \psi(\varphi(m)) \in \ker(\varphi)$, e isso implica que $m \in \ker(\varphi) + \mathrm{Im}(\psi)$. Logo $\ker(\varphi) + \mathrm{Im}(\psi) = M$.

Segue que M é a soma direta interna de $\ker(\varphi)$ e $\mathrm{Im}(\psi)$.

(c) Mostre que $\ker(\varphi)$ é finitamente gerado.

Como M é isomorfo à soma direta $\ker(\varphi) \oplus \mathrm{Im}(\psi)$, o módulo $\ker(\varphi) \cong M/\mathrm{Im}(\psi)$ é finitamente gerado porque M é finitamente gerado. Mais especificamente, se $m_1, \ldots, m_k$ geram M então geradores de $\ker(\varphi)$ são preimagens de $m_1 + \mathrm{Im}(\psi), \ldots, m_n + \mathrm{Im}(\psi)$ por meio do isomorfismo acima.

3. Seja $n \geq 1$ um inteiro e considere o $\mathbb{Z}$-módulo livre $M := \mathbb{Z}^n$. Sejam $b_i = (a_{i1}, \ldots, a_{in})$, $i = 1, \ldots, n$, elementos de M, e seja $E := \{b_1, \ldots, b_n\}$. Seja A a matriz quadrada $(a_{i,j})_{i,j=1,\ldots,n}$. Mostre que

   - E é linearmente independente (sobre $\mathbb{Z}$) se e somente se $\det(A) \neq 0$.
   - E é uma base de M se e somente se $\det(A) = \pm 1$.

   Suponha $\det(A) \neq 0$. Então E é linearmente independente sobre $\mathbb{Q}$, logo é obviamente linearmente independente sobre $\mathbb{Z}$ também.

   Suponha E linearmente independente sobre $\mathbb{Z}$. Para mostrar que $\det(A) \neq 0$ basta obviamente mostrar que E é linearmente independente sobre $\mathbb{Q}$, pois se isso vale então o resultado é um fato bem conhecido de álgebra linear sobre um corpo. Suponha que $\sum_{i=1}^n a_i b_i = 0$ com $a_i \in \mathbb{Q}$, escrevendo $a_i = x_i/y_i$, com $x_i, y_i \in \mathbb{Z}$ e $y_i \neq 0$, e multiplicando por $y_1 \cdots y_n$ obtemos que $\sum_{i=1}^n x_i t_i b_i = 0$ onde $t_i = (y_1 \cdots y_n)/y_i \in \mathbb{Z}$. Como E é linearmente independente sobre $\mathbb{Z}$, deduzimos que $x_i t_i = 0$ para todo $i = 1, \ldots, n$. Como $t_i \neq 0$, segue que $x_i = 0$, ou seja $a_i = 0$, para todo i.

   Suponha que E é uma base de M. Isso significa que todo elemento de M pode ser escrito de maneira única como $\sum_{i=1}^n a_i b_i$ com $a_i \in \mathbb{Z}$ para todo i. Seja e_i o i-esimo vetor da base canônica, o que tem 1 na i-esima componente e 0 nas outras. Existem $c_{ij} \in \mathbb{Z}$ tais que $e_i = \sum_{j=1}^n c_{ij} b_j$, seja C a matriz $(c_{ij})_{i,j}$. Por construção, $CA = 1$, ou seja o produto entre C e A é a matriz identidade. Segue que $1 = \det(CA) = \det(C)\det(A)$. Mas como todo coeficiente de A e de C é inteiro, $\det(A)$ e $\det(C)$ são inteiros. Segue que $\det(A) = \det(C) = \pm 1$.

Suponha que $\det(A) = \pm 1$. Então $\det(A) \neq 0$, logo A é uma matriz inversível em $\mathrm{GL}(n, \mathbb{Q})$, ou seja existe uma matriz $n \times n$ C com coeficientes racionais tal que $AC = 1$. A matriz C é obtida multiplicando $\det(A)^{-1}$ pela matriz dos cofatores, que são determinantes de oportunas submatrizes de A, multiplicados por ± 1. Em particular os coeficientes de C são inteiros, pois $\det(A)^{-1} = \pm 1$. Segue que E é um conjunto gerador de M pois todo vetor v é igual a $1v = ACv$ logo é combinação linear inteira das colunas de A, que são os elementos de E, e o conjunto E é linearmente independente sobre $\mathbb{Z}$ porque sendo $\det(A) = \pm 1 \neq 0$, E é linearmente independente sobre $\mathbb{Q}$. Segue que E é uma base do $\mathbb{Z}$-módulo M.

4. Sejam R um anel, M um R-módulo e N um R-submódulo de M. Mostre que se os R-módulos N e M/N são finitamente gerados então M é finitamente gerado. Vale o vice-versa?

   Se $n_1, \ldots, n_k$ geram N e $m_1 + N, \ldots, m_t + N$ geram M então $m_1, \ldots, m_t$, $n_1, \ldots, n_k$ geram M. De fato todo elemento $m \in M$ pertence a uma classe $\sum_{i=1}^{t} r_i m_i + N$, onde $r_i \in R$ para todo i, logo existe $n \in N$ tal que $m = n + \sum_{i=1}^{t} r_i m_i$, e $n \in N$ pode ser escrito como $n = \sum_{j=1}^{k} s_i n_i$, com $s_i \in R$ para todo i, logo $m = \sum_{j=1}^{k} s_i n_i + \sum_{i=1}^{t} r_i m_i$.

   O vice-versa não vale. Por exemplo considere $R = K[X_1, X_2, \ldots]$ o anel de polinômios sobre o corpo K em infinitas (númeraveis) variáveis. Seja M o ideal $(X_1, X_2, \ldots)$ de R. Então R é finitamente gerado como R-módulo pelo conjunto $\{1\}$, mas M não é finitamente gerado como R-módulo. De fato se $f_1, \ldots, f_k$ são elementos de M então existe um inteiro positivo n tal que X_n não aparece na escrita de nenhum dos polinômios f_j (cada um deles é expressão envolvendo um número finito de variáveis), logo X_n não pertence ao ideal de R gerado pelos f_j.

T3 – Trabalho semanal 3 de Álgebra Comutativa – Semestre 2021-2

Semana: 14 - 18 de fevereiro, 2022.
Prazo de entrega: 2 de março, 2022.

Cada um dos 4 itens vale 2.5 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Sejam I, J dois ideais do anel R. Mostre que existe um isomorfismo canônico de R-álgebras

$$R/I \otimes_R R/J \cong R/(I+J).$$

2. Considere os R-módulos livres $M = R^m$, $N = R^n$, $P = R^p$ e $Q = R^q$. Sejam $f : M \to N$, $g : P \to Q$ morfismos R-lineares. Como $M \otimes_R P \cong R^{mp}$ e $N \otimes_R Q \cong R^{nq}$, temos que $f \otimes g : M \otimes_R P \to N \otimes_R Q$ pode ser vista como função R-linear $R^{mp} \to R^{nq}$. Temos uma matriz A que representa f e uma matriz B que representa g, depois da escolha de uma base nos quatro módulos (que indicaremos com $\{e_i \ : \ i = 1, \ldots, k\}$ para $k \in \{m, n, p, q\}$). Mostre que a matriz de $f \otimes g$ nas bases

$$\{e_i \otimes e_j \ : \ i = 1, \ldots, m, \ j = 1, \ldots, p\} \qquad \text{de } M \otimes_R P,$$

$$\{e_i \otimes e_j \ : \ i = 1, \ldots, n, \ j = 1, \ldots, q\} \qquad \text{de } N \otimes_R Q,$$

é o *produto de Kronecker*

$$A \otimes B = \left(\begin{array}{c|c|c|c} a_{11}B & a_{12}B & \ldots & a_{1m}B \\ \hline a_{21}B & a_{22}B & \ldots & a_{2m}B \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{n1}B & a_{n2}B & \ldots & a_{nm}B \end{array}\right).$$

O traço de uma matriz é a soma dos elementos diagonais. Mostre que o traço de $A \otimes B$ é o produto entre os traços de A e de B.

3. Seja R um corpo. Considere o isomorfismo canônico $\varphi : R^2 \otimes_R R^2 \to R^4$. Mostre que os vetores de R^4 que são imagens de tensores simples de $R^2 \otimes_R R^2$ são exatamente os vetores (x, y, z, w) tais que $xw = yz$.

4. Seja

$$R = \mathbb{Q}[i] = \{a + ib \ : \ a, b \in \mathbb{Q}\} \subseteq \mathbb{C},$$

é um corpo. Mostre que o anel $R \otimes_{\mathbb{Q}} R$ (produto tensorial de $\mathbb{Q}$-álgebras) não é um corpo. Lembre-se que a multiplicação é induzida pela regra

$$(r_1 \otimes s_1) \cdot (r_2 \otimes s_2) := r_1 r_2 \otimes s_1 s_2.$$

Lembre também que $R \cong \mathbb{Q}[X]/(X^2 + 1)$.

T3 – Trabalho semanal 3 de Álgebra Comutativa – Resolução

1. Sejam I, J dois ideais do anel R. Mostre que existe um isomorfismo canônico de R-álgebras

$$R/I \otimes_R R/J \cong R/(I+J).$$

Sabemos que se M é um R-módulo então $M \otimes_R R/J \cong M/MJ$ (isomorfismo de R-módulos). Escolha $M = R/I$. Observe que

$$MJ = (R/I)J = (I+J)/I.$$

Isso é porque um elemento de $(R/I)J$ tem a forma $\sum_{t=1}^{k}(r_t + I)j_t = \sum_{t=1}^{k} r_t j_t + I$ para alguns $r_t \in R$, $j_t \in J$, ou seja tem a forma $j + I$ para algum $j \in J$. Segue que

$$\frac{R}{I} \otimes_R \frac{R}{J} = M \otimes_R \frac{R}{J} \cong \frac{M}{MJ} = \frac{R/I}{(I+J)/I} \cong \frac{R}{I+J}.$$

Chame essa composição de $\varphi : R/I \otimes_R R/J \to R/(I+J)$. Temos que $\varphi((r+I) \otimes (s+J)) = rs + I + J$. A multiplicação é preservada. De fato sejam $\overline{r_i} = r_i + I$, $\overline{s_i} = s_i + J$, então

$$\begin{aligned}\varphi(\overline{r_1} \otimes \overline{s_1} \cdot \overline{s_1} \otimes \overline{s_2}) &= \varphi(\overline{r_1 r_2} \otimes \overline{s_1 s_2}) = r_1 r_2 s_1 s_2 + I + J \\ &= (r_1 s_1 + I + J)(r_2 s_2 + I + J) \\ &= \varphi(\overline{r_1} \otimes \overline{s_1}) \cdot \varphi(\overline{r_2} \otimes \overline{s_2}).\end{aligned}$$

Como a multiplicação no produto tensorial de álgebras é obtido por extensão por bilinearidade dessa regra, isso mostra que φ é um isomorfismo de álgebras.

2. Considere os R-módulos livres $M = R^m$, $N = R^n$, $P = R^p$ e $Q = R^q$. Sejam $f : M \to N$, $g : P \to Q$ morfismos R-lineares. Como $M \otimes_R P \cong R^{mp}$ e $N \otimes_R Q \cong R^{nq}$, temos que $f \otimes g : M \otimes_R P \to N \otimes_R Q$ pode ser vista como função R-linear $R^{mp} \to R^{nq}$. Temos uma matriz A que representa f e uma matriz B que representa g, depois da escolha de uma base nos quatro módulos (que indicaremos com $\{e_i \ : \ i = 1, \ldots, k\}$ para $k \in \{m, n, p, q\}$). Mostre que a matriz de $f \otimes g$ nas bases

$$\{e_i \otimes e_j \ : \ i = 1, \ldots, m, \ j = 1, \ldots, p\} \qquad \text{de } M \otimes_R P,$$

$$\{e_i \otimes e_j \ : \ i = 1, \ldots, n, \ j = 1, \ldots, q\} \qquad \text{de } N \otimes_R Q,$$

é o *produto de Kronecker*

$$A \otimes B = \left(\begin{array}{c|c|c|c} a_{11}B & a_{12}B & \ldots & a_{1m}B \\ \hline a_{21}B & a_{22}B & \ldots & a_{2m}B \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{n1}B & a_{n2}B & \ldots & a_{nm}B \end{array}\right).$$

O traço de uma matriz é a soma dos elementos diagonais. Mostre que o traço de $A \otimes B$ é o produto entre os traços de A e de B.

Escrevendo $v = (v_1, \ldots, v_m) \in M$, $w = (w_1, \ldots, w_p) \in P$, temos

$$f(v) = Av = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} v_j \right) e_i,$$

$$g(w) = Bw = \sum_{r=1}^{q} \left(\sum_{k=1}^{p} b_{rk} w_k \right) e_r,$$

$$f(v) \otimes g(w) = Av \otimes Bw = \sum_{i,j,r,k} a_{ij} b_{rk} v_j w_k \cdot e_i \otimes e_r$$

Escolhendo $v = e_j$ e $w = e_k$, temos

$$f(e_j) \otimes g(e_k) = \sum_{i,r} a_{ij} b_{rk} \cdot e_i \otimes e_r.$$

Isso implica que as colunas da matriz de $f \otimes g$ na base dada pelos $e_j \otimes e_k$ são dadas pelos vetores seguintes, um abaixo do outro:

$$a_{1j} B_h, \ldots, a_{nj} B_h,$$

onde B_h é uma coluna de B, com $h = 1, \ldots, q$, e $j = 1, \ldots, m$.

3. Seja R um corpo. Considere o isomorfismo canônico

$$\varphi : R^2 \otimes_R R^2 \to R^4.$$

Mostre que os vetores de R^4 que são imagens de tensores simples de $R^2 \otimes_R R^2$ são exatamente os vetores (x, y, z, w) tais que $xw = yz$.

Defina $e_1 = (1, 0)$, $e_2 = (0, 1)$, elementos de R^2. Então $R^2 \otimes_R R^2$ é um espaço vetorial de dimensão 4 com base $e_i \otimes e_j$, $(i, j) \in \{1, 2\} \times \{1, 2\}$. Logo

$$\begin{aligned} \varphi((a, b) \otimes (c, d)) &= \varphi((ae_1 + be_2) \otimes (ce_1 + de_2)) \\ &= ac\varphi(e_1 \otimes e_1) + ad\varphi(e_1 \otimes e_2) \\ &\quad + bc\varphi(e_2 \otimes e_1) + bd\varphi(e_2 \otimes e_2). \end{aligned}$$

Na base $f_1 = \varphi(e_1 \otimes e_1)$, $f_2 = \varphi(e_1 \otimes e_2)$, $f_3 = \varphi(e_2 \otimes e_1)$, $f_4 = \varphi(e_2 \otimes e_2)$ de R^4 temos então

$$\varphi((a, b) \otimes (c, d)) = (ac, ad, bc, bd).$$

Observe que este vetor é do tipo (x, y, z, w) com $xw = yz$. Agora mostraremos a volta, ou seja que todo elemento $(x, y, z, w) \in R^4$ tal que $xw = yz$ é do tipo (ac, ad, bc, bd).

- Se $x \neq 0$ então sejam $a = 1$, $c = x$, $d = y$, $b = z/x$. Segue que $bd = zy/x = xw/x = w$.
- Se $x = 0$ então $yz = xw = 0$; se $y = 0$ sejam $a = 0$, $b = 1$, $c = z$, $d = w$; se $z = 0$ sejam $a = y$, $b = w$, $c = 0$, $d = 1$.

4. Seja
$$R = \mathbb{Q}[i] = \{a + ib \ : \ a, b \in \mathbb{Q}\} \subseteq \mathbb{C},$$
é um corpo. Mostre que o anel $R \otimes_{\mathbb{Q}} R$ (produto tensorial de $\mathbb{Q}$-álgebras) não é um corpo. Lembre-se que a multiplicação é induzida pela regra
$$(r_1 \otimes s_1) \cdot (r_2 \otimes s_2) := r_1 r_2 \otimes s_1 s_2.$$
Lembre também que $R \cong \mathbb{Q}[X]/(X^2 + 1)$.

Se S é uma R-álgebra, então temos um isomorfismo de S-álgebras
$$S \otimes_R \frac{R[X]}{I} \cong \frac{S[X]}{S[X]I}$$
onde $S[X]I$ é o ideal de $S[X]$ gerado por I. Isso pode ser mostrado usando a exatidão a direita do produto tensorial $- \otimes_R S$ aplicada à sequência exata de R-módulos
$$0 \longrightarrow I \longrightarrow R[X] \longrightarrow R[X]/I \longrightarrow 0$$
$$I \otimes_R S \longrightarrow R[X] \otimes_R S \longrightarrow R[X]/I \otimes_R S \longrightarrow 0$$
Agora observe que a imagem de $I \otimes_R S$ dentro $R[X] \otimes_R S \cong S[X]$ é exatamente $S[X]I$, o ideal de $S[X]$ gerado por I. Além disso, o morfismo $S[X] \to R[X]/I \otimes_R S$ é um homomorfismo sobrejetivo de S-álgebras. O resultado segue do teorema de isomorfismo.

Segue que
$$\begin{aligned}\mathbb{Q}[i] \otimes_{\mathbb{Q}} \mathbb{Q}[i] &\cong \mathbb{Q}[i] \otimes_{\mathbb{Q}} \frac{\mathbb{Q}[X]}{(X^2+1)} \cong \frac{\mathbb{Q}[i][X]}{(X^2+1)} \\ &\cong \frac{\mathbb{Q}[i][X]}{(X+i)} \times \frac{\mathbb{Q}[i][X]}{(X-i)} \cong \mathbb{Q}[i] \times \mathbb{Q}[i].\end{aligned}$$
Não é um corpo.

Para ver isso mais explicitamente, observe que as preimagens de $(0, 1)$ e de $(1, 0)$ são
$$a = 1 \otimes i + i \otimes 1,$$
$$b = 1 \otimes i - i \otimes 1,$$
e de fato é claro que $ab = 0$. Temos $a, b \neq 0$ pois eles têm imagens não nulas respectivamente por meio dos morfismos $\mathbb{Q}$-lineares
$$\varphi : \mathbb{Q}[i] \otimes_{\mathbb{Q}} \mathbb{Q}[i] \to \mathbb{Q}[i], \qquad \alpha \otimes \beta \mapsto \alpha \cdot \beta,$$
$$\psi : \mathbb{Q}[i] \otimes_{\mathbb{Q}} \mathbb{Q}[i] \to \mathbb{Q}[i], \qquad \alpha \otimes \beta \mapsto \alpha \cdot \overline{\beta},$$
onde $\overline{a + ib} = a - ib$. De fato $\varphi(a) = 2i \neq 0$ e $\psi(b) = -2i \neq 0$.

T4 – Trabalho semanal 4 de Álgebra Comutativa – Semestre 2021-2

Semana: 07 - 11 de março, 2022.
Prazo de entrega: 23 de março, 2022.

Cada um dos 5 itens vale 2 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Seja M um R-módulo Noetheriano e seja $f : M \to M$ um morfismo R-linear. Para todo inteiro $n \geq 1$ considere a composição f^n de f com si mesmo n vezes, se trata obviamente de um morfismo R-linear $M \to M$. Mostre que existe $n \geq 1$ tal que $\ker(f^n) \cap \mathrm{Im}(f^n) = \{0\}$.

2. Seja M um R-módulo Noetheriano e seja $f : M \to M$ um morfismo R-linear sobrejetivo. Mostre que f é injetivo. [Considere $\ker(f^n)$.]

3. Seja M um R-módulo Artiniano e seja $f : M \to M$ um morfismo R-linear injetivo. Mostre que f é sobrejetivo. [Considere $\mathrm{Im}(f^n)$.]

4. Encontre um anel não Noetheriano R tal que o localizado $R_{\mathfrak{p}}$ é Noetheriano para todo ideal primo $\mathfrak{p}$ de R.

5. Seja M um R-módulo Noetheriano e seja

$$I := (0 : M) = \{r \in R \ : \ rm = 0 \ \forall m \in M\} \trianglelefteq R.$$

   Mostre que R/I é um anel Noetheriano. [Dica: mostre que R/I é isomorfo, como R-módulo, a um R-submódulo de uma soma direta de um número finito de cópias de M.]

T4 – Trabalho semanal 4 de Álgebra Comutativa – Resolução

1. Seja M um R-módulo Noetheriano e seja $f : M \to M$ um morfismo R-linear. Para todo inteiro $n \geq 1$ considere a composição f^n de f com si mesmo n vezes, se trata obviamente de um morfismo R-linear $M \to M$. Mostre que existe $n \geq 1$ tal que $\ker(f^n) \cap \mathrm{Im}(f^n) = \{0\}$.

   A sequência $\ker(f^i)$ é não decrescente, no sentido que $\ker(f^i) \subseteq \ker(f^{i+1})$ para todo i. Como M é Noetheriano existe $n \in \mathbb{N}$ tal que $\ker(f^n) = \ker(f^m)$ para todo $m \geq n$. Afirmamos que $\ker(f^n) \cap \mathrm{Im}(f^n) = \{0\}$. Seja $x \in \ker(f^n) \cap \mathrm{Im}(f^n)$. Segue que $f^n(x) = 0$ e que existe $y \in M$ tal que $x = f^n(y)$. Logo $0 = f^n(x) = f^n(f^n(y)) = f^{2n}(y)$, o que implica que $y \in \ker(f^{2n}) = \ker(f^n)$. Segue que $x = f^n(y) = 0$.

2. Seja M um R-módulo Noetheriano e seja $f : M \to M$ um morfismo R-linear sobrejetivo. Mostre que f é injetivo. [Considere $\ker(f^n)$.]

   A sequência $\ker(f^i)$ é não decrescente, no sentido que $\ker(f^i) \subseteq \ker(f^{i+1})$ para todo i, logo existe $n \geq 1$ tal que $\ker(f^n) = \ker(f^{n+1})$ pois M é Noetheriano. Para mostrar que f é injetiva mostraremos que $\ker(f) = \{0\}$. Seja $m \in \ker(f)$, mostraremos que $m = 0$. Como f é sobrejetivo, f^n é sobrejetivo, logo existe $b \in M$ tal que $m = f^n(b)$. Segue que $0 = f(m) = f(f^n(b)) = f^{n+1}(b)$, logo $b \in \ker(f^{n+1}) = \ker(f^n)$, assim $m = f^n(b) = 0$.

3. Seja M um R-módulo Artiniano e seja $f : M \to M$ um morfismo R-linear injetivo. Mostre que f é sobrejetivo. [Considere $\mathrm{Im}(f^n)$.]

   A sequência $\mathrm{Im}(f^i)$ é não crescente, no sentido que $\mathrm{Im}(f^i) \supseteq \mathrm{Im}(f^{i+1})$ para todo i, logo existe $n \geq 1$ tal que $\mathrm{Im}(f^n) = \mathrm{Im}(f^m)$ para todo $m \geq n$, pois M é Artiniano. Seja $a \in M$, assim existe $b \in M$ tal que $f^{n+1}(b) = f^n(a)$, sendo $\mathrm{Im}(f^n) = \mathrm{Im}(f^{n+1})$. Segue que $f^n(a) = f^{n+1}(b) = f^n(f(b))$, logo $a = f(b)$, pois f^n é injetivo, sendo f injetivo.

4. Encontre um anel não Noetheriano R tal que o localizado $R_{\mathfrak{p}}$ é Noetheriano para todo ideal primo $\mathfrak{p}$ de R.

   Considere $R = F^{\mathbb{N}}$ onde $F = \mathbb{Z}/2\mathbb{Z}$. R é o anel das funções $\mathbb{N} \to F$, com as operações por componentes. Para todo $B \subseteq \mathbb{N}$ defina

   $$I_B := \{f \in R \ : \ f(i) = 0 \quad \forall i \in B\},$$

   é um ideal de R. Definindo $B_i = \mathbb{N} - \{1, \ldots, i\}$ para $i \in \mathbb{N}$ deduzimos que R não é Noetheriano pois admite a seguente sequência infinita de ideais.

   $$I_{B_1} \subset I_{B_2} \subset I_{B_3} \subset \ldots$$

   Seja $\mathfrak{p}$ um ideal primo de R. Como $r^2 = r$ para todo $r \in R$, no localizado $R_{\mathfrak{p}}$ temos $(r/s)^2 = r^2/s^2 = r/s$, logo $x^2 = x$, ou seja $x(x-1) = 0$, para todo $x \in R_{\mathfrak{p}}$. Se existe $x \in R_{\mathfrak{p}}$ diferente de 0 e de 1 então x e $x - 1$ são não nulos e não inversíveis, porém $x - (x - 1) = 1$ é inversível. Mas em

um anel local os elementos não inversíveis formam um ideal. Deduzimos uma contradição, logo $R_{\mathfrak{p}}$ é um corpo com dois elementos. Em particular é um anel Noetheriano.

5. Seja M um R-módulo Noetheriano e seja

$$I := (0 : M) = \{r \in R \ : \ rm = 0 \quad \forall m \in M\} \trianglelefteq R.$$

Mostre que R/I é um anel Noetheriano. [Dica: mostre que R/I é isomorfo, como R-módulo, a um R-submódulo de uma soma direta de um número finito de cópias de M.]

Sejam $m_1, \ldots, m_n$ geradores do R-módulo M. Considere

$$f : R \to M^n \qquad f(r) := (rm_1, \ldots, rm_n).$$

Se trata de um morfismo R-linear cujo núcleo é I. Logo R/I é isomorfo a um submódulo de M^n, logo é um R-módulo Noetheriano, pois M^n é um R-módulo Noetheriano, sendo uma soma direta de R-módulos Noetherianos. Mas é claro que R/I é Noetheriano como R-módulo se e somente se é Noetheriano como anel. Logo R/I é um anel Noetheriano.

T5 – Trabalho semanal 5 de Álgebra Comutativa – Semestre 2021-2

Semana: 14 - 18 de março, 2022.
Prazo de entrega: 30 de março, 2022.

Cada um dos 5 itens vale 2 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Seja R um anel e seja S um subconjunto de R contendo 1 e multiplicativamente fechado. Mostre que se M é um R-módulo Noetheriano então $S^{-1}M$ é um $S^{-1}R$-módulo Noetheriano.

2. Seja $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$ e seja $P(X)$ o polinômio minimal de α sobre $\mathbb{Q}$, ou seja o único polinômio mônico irredutível de $\mathbb{Q}[X]$ que tem α como raiz. Mostre que α é um inteiro algébrico (i.e. é raíz de um polinômio mônico com coeficientes inteiros) se e somente se $P(X) \in \mathbb{Z}[X]$.

3. Seja K um corpo algebricamente fechado, sejam A, B duas K-álgebras finitamente geradas e seja $f : A \to B$ um morfismo de K-álgebras. Mostre que se $\mathfrak{m}$ é um ideal maximal de B então a preimagem $f^{\leftarrow}(\mathfrak{m})$ é um ideal maximal de A.

4. Fatore os ideais principais (30), (23), (29), (82) do anel $\mathbb{Z}[\sqrt{-5}]$ como produto de ideais maximais. Faça a mesma coisa em $\mathbb{Z}[\sqrt{-6}]$.

5. Seja $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\}$. Mostre que o grupo $U(R)$ dos elementos inversíveis de R é isomorfo ao produto direto dos grupos multiplicativos cíclicos $\langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$.

T5 – Trabalho semanal 5 de Álgebra Comutativa – Resolução

1. Seja R um anel e seja S um subconjunto de R contendo 1 e multiplicativamente fechado. Mostre que se M é um R-módulo Noetheriano então $S^{-1}M$ é um $S^{-1}R$-módulo Noetheriano.

   Os $S^{-1}R$-submódulos de $S^{-1}M$ são do tipo $S^{-1}N$ para algum R-submódulo N de M. De fato, seja L um $S^{-1}R$-submódulo de $S^{-1}M$ e seja

   $$N := \{r \in R \ : \ \exists s \in S \text{ tal que } r/s \in L\}.$$

   É claro que $L \subseteq S^{-1}N$. Se $r \in N$ então existe $s \in S$ tal que $r/s \in L$, logo se $t \in S$ então $r/t = (r/s)(s/t) \in L$, isso mostra que $S^{-1}N \subseteq L$. Além disso N é um R-submódulo de M.

   Se $L = S^{-1}N$ é um $S^{-1}R$-submódulo de $S^{-1}M$ então N é finitamente gerado como R-módulo por $n_1, \ldots, n_r$, assim $S^{-1}N$ é gerado como $S^{-1}R$-módulo por $n_1/1, \ldots, n_r/1$.

2. Seja $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$ e seja $P(X)$ o polinômio minimal de α sobre $\mathbb{Q}$, ou seja o único polinômio mônico irredutível de $\mathbb{Q}[X]$ que tem α como raiz. Mostre que α é um inteiro algébrico (i.e. é raíz de um polinômio mônico com coeficientes inteiros) se e somente se $P(X) \in \mathbb{Z}[X]$.

   Se $P(X) \in \mathbb{Z}[X]$ então α, sendo raiz de $P(X)$, é um inteiro algébrico. Agora suponha que α é um inteiro algébrico, assim existe $L(X) \in \mathbb{Z}[X]$, mônico, tal que $L(\alpha) = 0$. Como $\mathbb{Z}[X]$ é um domínio de fatoração única, existe um fator irredutível $L_0(X)$ de $L(X)$ em $\mathbb{Z}[X]$ tal que $L_0(\alpha) = 0$. Como $L(X)$ é mônico, segue que $\pm L_0(X)$ é mônico, logo é um polinômio primitivo (o maior divisor comum dos seus coeficientes é 1), assim $L_0(X)$ é irredutível em $\mathbb{Q}[X]$ pelo lema de Gauss. Pela unicidade do polinômio minimal, segue que $P(X) = \pm L_0(X) \in \mathbb{Z}[X]$.

3. Seja K um corpo algebricamente fechado, sejam A, B duas K-álgebras finitamente geradas e seja $f : A \to B$ um morfismo de K-álgebras. Mostre que se $\mathfrak{m}$ é um ideal maximal de B então a preimagem $f^{\leftarrow}(\mathfrak{m})$ é um ideal maximal de A.

   Seja $\mathfrak{p} := f^{\leftarrow}(\mathfrak{m})$, então temos o homomorfismo induzido de K-álgebras $\alpha : K \to A/\mathfrak{p}$ e $\beta : A/\mathfrak{p} \to B/\mathfrak{m}$, injetivos. Observe que $B/\mathfrak{m}$ é um corpo e uma K-álgebra finitamente gerada, logo é finitamente gerada como K-módulo (K-espaço vetorial) pelo lema de Zariski. Como K é algebricamente fechado, segue que a composição $\beta \circ \alpha : K \to B/\mathfrak{m}$ é um isomorfismo, em particular é sobrejetivo, logo β é sobrejetivo. Por outro lado β é obviamente injetivo, logo é um isomorfismo e $A/\mathfrak{p} \cong B/\mathfrak{m}$ é um corpo, ou seja $\mathfrak{p}$ é um ideal maximal de A.

4. Fatore os ideais principais (30), (23), (29), (82) do anel $\mathbb{Z}[\sqrt{-5}]$ como produto de ideais maximais. Faça a mesma coisa em $\mathbb{Z}[\sqrt{-6}]$.

No caso de $R = \mathbb{Z}[\sqrt{-5}]$ seja $\alpha = \sqrt{-5}$. As fatorações são obtidas fatorando X^2+5 módulo p, onde $p \in \mathbb{Z}$ é um primo que aparece na fatoração, como visto nas aulas teóricas.

$(30) = (2) \cdot (3) \cdot (5) = (2, \alpha+1)^2 \cdot (3, \alpha+1) \cdot (3, \alpha+2) \cdot (5, \alpha)^2$.

$(23) = (23, \alpha+8) \cdot (23, \alpha+15)$.

$(29) = (29, \alpha+13) \cdot (29, \alpha+16)$.

$(82) = (2) \cdot (41) = (2, \alpha+1)^2 \cdot (41, \alpha+6) \cdot (41, \alpha+35)$

No caso de $R = \mathbb{Z}[\sqrt{-6}]$ seja $\beta = \sqrt{-6}$. As fatorações são obtidas fatorando X^2+6 módulo p, onde $p \in \mathbb{Z}$ é um primo que aparece na fatoração, como visto nas aulas teóricas.

$(30) = (2) \cdot (3) \cdot (5) = (2, \beta)^2 \cdot (3, \beta)^2 \cdot (5, \beta+2) \cdot (5, \beta+3)$.

(23) é maximal pois X^2+6 é irredutível em $\mathbb{F}_{23}[X]$.

$(29) = (29, \beta+9) \cdot (29, \beta+20)$.

$(82) = (2, \beta)^2 \cdot (41)$.

5. Seja $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\}$. Mostre que o grupo $U(R)$ dos elementos inversíveis de R é isomorfo ao produto direto dos grupos multiplicativos cíclicos $\langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$.

   Como vimos nas aulas teóricas, $a + b\sqrt{2}$ é uma unidade se e somente se a sua norma é ± 1, ou seja $a^2 - 2b^2 = \pm 1$, em particular $a \neq 0$. Se $b = 0$ então $a + b\sqrt{2} = \pm 1$. Suponha $b \neq 0$. Sejam $\alpha = 1 + \sqrt{2}$, $G := \langle \alpha \rangle$ e suponha que existam unidades de R fora de $\langle -1 \rangle G = G \cup (-G)$, por contradição.

   Seja $a + b\sqrt{2}$ uma unidade de R não pertencente a $\langle -1 \rangle G$. Temos $a \neq 0$ e $-a - b\sqrt{2} \notin \langle -1 \rangle G$, logo podemos supor $a > 0$.

   $$U(R) \ni t = (a + b\sqrt{2}) \cdot \alpha^{-1} = (a + b\sqrt{2})(\sqrt{2} - 1) = (2b - a) + (a - b)\sqrt{2}.$$

   Suponha $b > 0$ mínimo tal que $a + b\sqrt{2} \in U(R) \setminus \langle -1 \rangle G$. Temos $\pm 1 = N(a + b\sqrt{2}) = a^2 - 2b^2$, logo $b^2 < a^2 = 2b^2 \pm 1 < 4b^2$, logo $b < a < 2b$, ou seja $0 < a - b < b$, logo $t = (2b - a) + (a - b)\sqrt{2} \in \langle -1 \rangle G$ por minimalidade de b, assim t é igual a um elemento do tipo $\pm\alpha^n$. Segue que $a + b\sqrt{2} = \pm\alpha^n \cdot (\sqrt{2} - 1)^{-1} = \pm\alpha^{n+1} \in \langle -1 \rangle G$.

   Suponha $b < 0$ e a mínimo tal que $a + b\sqrt{2} \in U(R) \setminus \langle -1 \rangle G$. Como $b^2 < a^2 < 4b^2$ pelo argumento acima, deduzimos que $-b < a < -2b$, assim $0 < -a - 2b < a$. Observe que

   $$U(R) \ni s = -(a+b\sqrt{2}) \cdot \alpha = -(a+b\sqrt{2})(1+\sqrt{2}) = (-a-2b)+(-a-b)\sqrt{2},$$

   e sendo $0 < -a - 2b < a$ e $-a - b < 0$, deduzimos que $s = \pm\alpha^n$ para algum $n \in \mathbb{Z}$ por minimalidade de a. Segue que $a + b\sqrt{2} = \pm\alpha^{n-1}$.

T6 – Trabalho semanal 6 de Álgebra Comutativa – Semestre 2021-2

Semana: 21 - 25 de março, 2022.
Prazo de entrega: 6 de abril, 2022.

Cada um dos 4 itens vale 2,5 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Seja R um anel Noetheriano. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).
   (a) Seja I um ideal primo de R. Então I é irredutível.
   (b) Seja I um ideal irredutível de R. Então $\sqrt{I}$ é irredutível.
   (c) Seja I um ideal irredutível de R. Então $\sqrt{I}$ é primo.
   (d) Seja I um ideal irredutível de R. Então I é primo.
   (e) Seja I um ideal primo de R. Então I^2 é irredutível.

2. Seja I um ideal próprio de R tal que
   (*) para todo $J_1, J_2 \trianglelefteq R$, se $J_1 \cap J_2 \subseteq I$ então $J_1 \subseteq I$ ou $J_2 \subseteq I$.
   (a) Mostre que se $\sqrt{I} = I$ então I é um ideal primo.
   (b) O ideal (X, Y^2) de $\mathbb{Q}[X, Y]$ satisfaz (*)?
   (c) O ideal (X, Y^2) de $\mathbb{Q}[X, Y]$ é irredutível?

3. Mostre que o ideal $(4, X)$ de $R = \mathbb{Z}[X]$ é $(2, X)$-primário (ou seja é primário e $\sqrt{(4, X)} = (2, X)$) mas não é uma potência de $(2, X)$.

4. Seja L uma extensão finita de $\mathbb{Q}$, de grau n, seja D o anel dos inteiros de L (i.e. um elemento de L pertence a D se e somente se é raiz de um polinômio mônico de $\mathbb{Z}[X]$) e seja $\alpha \in L$. Considere $f_\alpha : L \to L$ definido por $f_\alpha(x) := \alpha x$. Seja $T(\alpha)$ o traço de f_α, i.e. o traço (a soma dos elementos diagonais) da matriz $n \times n$ que representa f_α em uma base de L sobre $\mathbb{Q}$ (esta definição não depende da base escolhida). Seja $P(X) = \sum_{i=0}^{d} a_i X^i$ o polinômio minimal de α sobre $\mathbb{Q}$. Mostre que

$$T(\alpha) = -\frac{n}{d} \cdot a_{d-1}.$$

   Deduza que se $\alpha \in D$ então $T(\alpha) \in \mathbb{Z}$. Vale a volta?

T6 – Trabalho semanal 6 de Álgebra Comutativa – Resolução

1. Seja R um anel Noetheriano. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).

   (a) Seja I um ideal primo de R. Então I é irredutível. Verdadeiro. Se $I = A \cap B$ com A, B ideais de R então $I \supseteq A \cap B$ e I é primo, logo I contém A ou B, logo é igual a A ou B pois está contido em ambos.

   (b) Seja I um ideal irredutível de R. Então $\sqrt{I}$ é irredutível. Verdadeiro. De fato, em um anel Noetheriano todo ideal irredutível é primário, logo I é primário, logo $\sqrt{I}$ é primo, em particular é irredutível.

   (c) Seja I um ideal irredutível de R. Então Então $\sqrt{I}$ é primo. Verdadeiro. De fato, como I é irredutível e R é Noetheriano, I é primário, logo $\sqrt{I}$ é primo.

   (d) Seja I um ideal irredutível de R. Então I é primo. Falso, por exemplo (4) é um ideal irredutível de $\mathbb{Z}$ e não é primo, pois se n, m são inteiros positivos com $(4) = (n) \cap (m) = (\text{mmc}(n, m))$ então $\text{mmc}(n, m) = 4$ logo $n = 4$ ou $m = 4$.

   (e) Seja I um ideal primo de R. Então I^2 é irredutível. Falso, pois em um anel Noetheriano todo ideal irredutível é primário e já vimos um exemplo em que o quadrado de um ideal primo não é primário: considere o ideal I de $K[X, Y, Z]/(XY - Z^2)$ gerado por x, z, sendo $x = X + (XY - Z^2)$ e $y = Y + (XY - Z^2)$. Já vimos que I^2 contém $z^2 = xy$ mas não contém x e não contém y^n para nenhum n.

2. Seja I um ideal próprio de R tal que

   (*) para todo $J_1, J_2 \trianglelefteq R$, se $J_1 \cap J_2 \subseteq I$ então $J_1 \subseteq I$ ou $J_2 \subseteq I$.

   (a) Mostre que se $\sqrt{I} = I$ então I é um ideal primo.

   (b) O ideal (X, Y^2) de $\mathbb{Q}[X, Y]$ satisfaz (*)?

   (c) O ideal (X, Y^2) de $\mathbb{Q}[X, Y]$ é irredutível?

   Se $xy \in I$ então $(x)(y) \subseteq I$, logo $(x) \cap (y) \subseteq \sqrt{(x) \cap (y)} = \sqrt{(x)(y)} \subseteq \sqrt{I} = I$, logo $(x) \subseteq I$ ou $(y) \subseteq I$, ou seja $x \in I$ ou $y \in I$.

   $(X + Y)Y \in (X, Y^2)$, $X + Y \notin (X, Y^2)$, $Y \notin (X, Y^2)$ logo (X, Y^2) não satisfaz (*) pois contém $(X + Y) \cap (Y)$ mas não contém $(X + Y)$, (Y).

   Observe que (X, Y^2) é irredutível em $\mathbb{Q}[X, Y]$ se e somente se $(X, Y^2)/(X)$ é irredutível em $\mathbb{Q}[X, Y]/(X)$, se e somente se (Y^2) é irredutível em $\mathbb{Q}[Y]$, o que é verdade.

3. Mostre que o ideal $(4, X)$ de $R = \mathbb{Z}[X]$ é $(2, X)$-primário (ou seja é primário e $\sqrt{(4, X)} = (2, X)$) mas não é uma potência de $(2, X)$.

   Seja $I = (4, X)$. Temos $2^2 \in I$ e $X \in I$, logo $2, X \in \sqrt{I}$, logo $(2, X) \subseteq \sqrt{I}$. Por outro lado $(2, X)$ é um ideal maximal de $R = \mathbb{Z}[X]$, logo temos

igualdade (pois $\sqrt{I} \neq R$, sendo $I \neq R$). Como $\sqrt{I}$ é um ideal maximal, segue que I é primário. Por outro lado I não é uma potência de $(2, X)$ porque $X \in I$ mas $X \notin (2, X)^2$.

4. Seja L uma extensão finita de $\mathbb{Q}$, de grau n, seja D o anel dos inteiros de L (i.e. um elemento de L pertence a D se e somente se é raiz de um polinômio mônico de $\mathbb{Z}[X]$) e seja $\alpha \in L$. Considere $f_\alpha : L \to L$ definido por $f_\alpha(x) := \alpha x$. Seja $T(\alpha)$ o traço de f_α, i.e. o traço (a soma dos elementos diagonais) da matriz $n \times n$ que representa f_α em uma base de L sobre $\mathbb{Q}$ (esta definição não depende da base escolhida). Seja $P(X) = \sum_{i=0}^{d} a_i X^i$ o polinômio minimal de α sobre $\mathbb{Q}$. Mostre que

$$T(\alpha) = -\frac{n}{d} \cdot a_{d-1}.$$

Deduza que se $\alpha \in D$ então $T(\alpha) \in \mathbb{Z}$. Vale a volta?

No caso $L = \mathbb{Q}(\alpha)$, temos que a matriz de f_α na base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ de L sobre $\mathbb{Q}$ é

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{d-1} \end{pmatrix}.$$

Logo $T(\alpha) = -a_{d-1}$. Neste caso $n = d$.

No caso geral, seja $\{v_1, \ldots, v_t\}$ uma base de L sobre $\mathbb{Q}(\alpha)$, onde $t = |L : \mathbb{Q}(\alpha)|$. Pela formula do grau

$$n = |L : \mathbb{Q}| = |L : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}| = td,$$

logo $t = n/d$. A matriz de f_α na base $\{\alpha^i v_j \ : \ i = 1, \ldots, d, \ t = 1, \ldots, t\}$ é a matriz em blocos

$$\begin{pmatrix} A & 0 & \ldots & 0 \\ 0 & A & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A \end{pmatrix}$$

Logo o seu traço é $t \cdot (-a_{d-1})$.

T7 – Trabalho semanal 7 de Álgebra Comutativa – Semestre 2021-2

Semana: 28 de março - 01 de abril, 2022.
Prazo de entrega: 13 de abril, 2022.

Cada um dos 5 itens vale 2 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Seja R um domínio de Dedekind.

   (a) Mostre que se R contém apenas um número finito de ideais primos então todos os ideais de R são principais.

   [Dica. Se $\mathfrak{p}$ é um ideal primo não nulo de R, construa um oportuno elemento $r \in \mathfrak{p} - \mathfrak{p}^2$ e mostre que $\mathfrak{p} = (r)$.]

   (b) Seja n um inteiro maior que 1. Construa um domínio de Dedekind com exatamente n ideais primos.

   [Dica. Localize $\mathbb{Z}$ oportunamente.]

2. Seja R um domínio de Dedekind, seja $\mathfrak{p} \in \mathrm{Spec}(R)$ e seja I um ideal de R. Mostre que se $\mathfrak{p}I = I$ então $I = \{0\}$.

3. Seja $\alpha = \sqrt[3]{10} \in \mathbb{R}$. Mostre que o anel dos inteiros de $\mathbb{Q}(\alpha)$ não é $\mathbb{Z}[\alpha]$. Lembre-se que o anel dos inteiros de $\mathbb{Q}(\alpha)$ é o conjunto dos elementos de $\mathbb{Q}(\alpha)$ que são raízes de polinômios mônicos com coeficientes inteiros.

   [Dica. Considere $\beta = (1 + \alpha + \alpha^2)/3$.]

4. Seja R um anel local com ideal maximal $\mathfrak{m}$, sejam M, N dois R-módulos finitamente gerados e seja $f : M \to N$ um morfismo R-linear. Mostre que se o morfismo induzido $M/\mathfrak{m}M \to N/\mathfrak{m}N$ é sobrejetivo, então f é sobrejetivo.

   [Dica. Tensorize com $R/\mathfrak{m}$ sobre R.]

5. Seja R um anel local e sejam M, N dois R-módulos finitamente gerados. Suponha que $M \otimes_R N = \{0\}$. Mostre que $M = \{0\}$ ou $N = \{0\}$.

   [Dica. Seja $\mathfrak{m}$ o ideal maximal de R e seja $K = R/\mathfrak{m}$. Tensorize $M \otimes_R N$ com K sobre R.]

Pode usar o lema de Nakayama (veja as notas de aula).

T7 – Trabalho semanal 7 de Álgebra Comutativa – Resolução

1. Seja R um domínio de Dedekind.

   (a) Mostre que se R contém apenas um número finito de ideais primos então todos os ideais de R são principais.

   [Dica. Se $\mathfrak{p}$ é um ideal primo não nulo de R, construa um oportuno elemento $r \in \mathfrak{p} - \mathfrak{p}^2$ e mostre que $\mathfrak{p} = (r)$.]

   (b) Seja n um inteiro maior que 1. Construa um domínio de Dedekind com exatamente n ideais primos.

   [Dica. Localize oportunamente.]

   Suponha que R tenha apenas um número finito de ideais primos, $\mathfrak{p} = \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$. Pela unicidade da fatoração $\mathfrak{p}_1 \neq \mathfrak{p}_1^2$, logo existe $x \in \mathfrak{p}_1 - \mathfrak{p}_1^2$. Temos

   $$\frac{R}{\mathfrak{p}_1^2\mathfrak{p}_2 \cdots \mathfrak{p}_n} \cong \frac{R}{\mathfrak{p}_1^2} \times \frac{R}{\mathfrak{p}_2} \times \ldots \times \frac{R}{\mathfrak{p}_n},$$

   logo existe $r \in R$ tal que $r + \mathfrak{p}_1^2 = x + \mathfrak{p}_1^2$ e $r + \mathfrak{p}_i = 1 + \mathfrak{p}_i$ para todo $i = 2, \ldots, n$. Segue que o único ideal maximal de R que contém o ideal principal (r) é $\mathfrak{p}_1$, logo a fatoração de (r) é $\mathfrak{p}_1^m$ para algum m. Por outro lado $r \notin \mathfrak{p}_1^2$, logo $m = 1$ e $\mathfrak{p}_1 = (r)$. Isso mostra que todos os ideais primos de R são principais. Como todo ideal não nulo de R é um produto de ideais primos, todos os ideais são principais.

   Sejam $p_1, \ldots, p_{n-1}$ números primos distintos e seja S o conjunto dos inteiros coprimos com todos os p_i. Então S é multiplicativamente fechado e os ideais primos de $S^{-1}\mathbb{Z}$ são do tipo $S^{-1}I$ onde I é um ideal primo de $\mathbb{Z}$ disjunto de S, ou seja são $\{0\}$ e $S^{-1}(p_i\mathbb{Z})$, $i = 1, \ldots, n-1$. Segue que $S^{-1}\mathbb{Z}$ admite exatamente n ideais primos, e é um domínio de Dedekind pois é um localizado de um domínio de Dedekind (veja as notas de aula).

2. Seja R um domínio de Dedekind, seja $\mathfrak{p} \in \mathrm{Spec}(R)$ e seja I um ideal não nulo de R. Mostre que se $\mathfrak{p}I = I$ então $I = \{0\}$.

   Segue imediatamente da unicidade da fatoração de um ideal não nulo como produto de ideais primos. Explicitamente, suponha $I \neq \{0\}$ por contradição, então I é produto de ideais primos de maneira única, digamos $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ com os $\mathfrak{p}_i$ ideais primos. Como $\mathfrak{p}I = I$, temos duas fatorações distintas de I, $\mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n = I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, contradição. É também possível localizar e usar o lema de Nakayama.

3. Seja $\alpha = \sqrt[3]{10} \in \mathbb{R}$. Mostre que o anel dos inteiros de $\mathbb{Q}(\alpha)$ não é $\mathbb{Z}[\alpha]$. Lembre-se que o anel dos inteiros de $\mathbb{Q}(\alpha)$ é o conjunto dos elementos de $\mathbb{Q}(\alpha)$ que são raízes de polinômios mônicos com coeficientes inteiros.

   [Dica. Considere $\beta = (1 + \alpha + \alpha^2)/3$.]

   Temos $\beta(\alpha - 1) = (\alpha^3 - 1)/3 = 9/3 = 3$, logo $\beta = 3/(\alpha - 1)$. Temos

   $$(\alpha - 1)^3 = \alpha^3 - 3\alpha^2 + 3\alpha - 1 = 9 - 3\alpha(\alpha - 1) = 9 - 9\alpha/\beta = 9(1 - \alpha/\beta).$$

Segue que

$$\beta^3 = (3/(\alpha-1))^3 = \frac{27}{9(1-\alpha/\beta)} = \frac{3\beta}{\beta-\alpha},$$

logo $\beta^2(\beta-\alpha) = 3$. Usando $\alpha = 1 + 3/\beta$ obtemos que

$$3 = \beta^2(\beta-\alpha) = \beta^2(\beta-1-3/\beta) = \beta^3 - \beta^2 - 3\beta,$$

logo β pertence ao anel dos inteiros de $\mathbb{Q}(\alpha)$ mas não pertence a $\mathbb{Z}[\alpha]$.

4. Seja R um anel local com ideal maximal $\mathfrak{m}$, sejam M, N dois R-módulos finitamente gerados e seja $f : M \to N$ um morfismo R-linear. Mostre que se o morfismo induzido $M/\mathfrak{m}M \to N/\mathfrak{m}N$ é sobrejetivo, então f é sobrejetivo.

   [Dica. Tensorize com $R/\mathfrak{m}$ sobre R.]

   Seja $A = \operatorname{coker}(f) = N/f(M)$. Queremos mostrar $A = \{0\}$, e pelo lema de Nakayama basta mostrar que $\mathfrak{m}A = A$. Tensorizando

   $$0 \to M \to N \to A \to 0$$

   com $R/\mathfrak{m}$ temos a sequência exata

   $$M/\mathfrak{m}M \to N/\mathfrak{m}N \to A/\mathfrak{m}A \to 0$$

   Logo o núcleo de $h : N/\mathfrak{m}N \to A/\mathfrak{m}A$ é a imagem de $M/\mathfrak{m}M$, ou seja $N/\mathfrak{m}N$, em outras palavras $h = 0$. Mas como h é sobrejetiva, segue $A = \mathfrak{m}A$.

5. Seja R um anel local e sejam M, N dois R-módulos finitamente gerados. Suponha que $M \otimes_R N = \{0\}$. Mostre que $M = \{0\}$ ou $N = \{0\}$.

   [Dica. Seja $\mathfrak{m}$ o ideal maximal de R e seja $K = R/\mathfrak{m}$. Tensorize $M \otimes_R N$ com K sobre R.]

   Temos

   $$\{0\} = (M \otimes_R N) \otimes_R K \cong (M \otimes_R K) \otimes_K (N \otimes_R K).$$

   Como $M \otimes_R K$ e $N \otimes_R K$ são espaços vetoriais, temos que $M/\mathfrak{m}M \cong M \otimes_R K = \{0\}$ ou $N/\mathfrak{m}N \cong N \otimes_R K = \{0\}$. Pelo lema de Nakayama segue $M = \{0\}$ ou $N = \{0\}$.

T8 – Trabalho semanal 8 de Álgebra Comutativa – Semestre 2021-2

Semana: 04 - 08 de abril, 2022.
Prazo de entrega: 20 de abril, 2022.

Cada um dos 5 itens vale 2 pontos. Justifique todas as respostas.
Todos os aneis considerados são comutativos e unitários.

1. Sejam I, J dois ideais de R. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).
   (a) $\sqrt{I+J} = \sqrt{I} + \sqrt{J}$.
   (b) Se I e J são ideais radicais então $I + J$ é radical.

2. Para cada um dos aneis seguintes, diga se é um corpo.

$$\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}), \qquad \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}), \qquad \mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[i].$$

3. Seja I o ideal principal de $\mathbb{C}[X, Y]$ gerado por $X^2 - Y^2 - 1$. Mostre que todo ideal maximal de $\mathbb{C}[X, Y]/I$ é do tipo $(X - a, Y - b)/I$ com $a, b \in \mathbb{C}$ tais que $a^2 = b^2 + 1$. Isso vale também com $\mathbb{R}$ no lugar de $\mathbb{C}$?

4. Seja K um corpo. Considere $R := K[X, Y]/I$ onde $I = (XY - 1)$.
   (a) Mostre que se A é um domínio de ideais principais (PID) e S é um subconjunto de A contendo 1 e multiplicativamente fechado então o localizado $S^{-1}A$ é um domínio de ideais principais (PID).
   (b) Mostre que R é um domínio de ideais principais (PID). [Dica. Observe que R é isomorfo a um localizado de $K[X]$ (qual?).]
   (c) Deduza que R é um domínio de Dedekind. [Dica. Mostre que um PID tem dimensão no máximo 1.]
   (d) Sejam $x := X + I$, $y := Y + I$, elementos de R. Fatore os ideais principais $(x-2)$, $(y-1)$, $(x-y)$, $(x+y-2)$ de R como produtos de ideais primos de R. [Dica. Faça um desenho das curvas envolvidas.]

5. Seja K uma extensão finita de $\mathbb{Q}$, ou seja $\mathbb{Q}$ é um subcorpo de K e a dimensão $|K : \mathbb{Q}| = \dim_{\mathbb{Q}}(K)$ é finita. Seja R o anel dos inteiros de K, ou seja R é o conjunto dos elementos de K que são raízes de polinômios mônicos de $\mathbb{Z}[X]$. Seja I um ideal não nulo de R. Mostre que R/I é um anel finito.

   [Dica. Lembre-se que R é finitamente gerado como $\mathbb{Z}$-módulo.]

   É verdade que se D é um domínio de Dedekind qualquer e $\{0\} \neq I \trianglelefteq D$ então D/I é sempre um anel finito?

T8 – Trabalho semanal 8 de Álgebra Comutativa – Resolução

1. Sejam I, J dois ideais de R. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).

   (a) $\sqrt{I+J} = \sqrt{I} + \sqrt{J}$.

   (b) Se I e J são ideais radicais então $I + J$ é radical.

   Em $\mathbb{Q}[X, Y]$ temos

   $$\sqrt{(Y) + (Y - X^2)} = \sqrt{(X^2, Y)} = (X, Y)$$
   $$\sqrt{(Y)} + \sqrt{(Y - X^2)} = (Y) + (Y - X^2) = (X^2, Y).$$

   Isso dá um contra-exemplo aos dois itens, logo são ambos falsos.

2. Para cada um dos aneis seguintes, diga se é um corpo.

   $$\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}), \qquad \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}), \qquad \mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[i].$$

   Temos que

   $$\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[3]{2})[X]/(X^4 - 2)$$

   é um corpo pois $X^4 - 2$ é irredutível em $\mathbb{Q}(\sqrt[3]{2})[X]$.

   $$\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{R}[X]/(X^3 - 2)$$

   não é um corpo pois $X^3 - 2$ é redutível em $\mathbb{R}[X]$, um fator irredutível dele é $X - \sqrt[3]{2} \in \mathbb{R}[X]$.

   $$\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[i] \cong \mathbb{Z}[\sqrt{2}][X]/(X^2 + 1) \cong \mathbb{Z}[\sqrt{2}, i]$$

   não é um corpo pois contém 2 mas não contém $1/2$.

3. Seja I o ideal principal de $\mathbb{C}[X, Y]$ gerado por $X^2 - Y^2 - 1$. Mostre que todo ideal maximal de $\mathbb{C}[X, Y]/I$ é do tipo $(X - a, Y - b)/I$ com $a, b \in \mathbb{C}$ tais que $a^2 = b^2 + 1$. Isso vale também com $\mathbb{R}$ no lugar de $\mathbb{C}$?

   Como $\mathbb{C}$ é algebricamente fechado, todo ideal maximal de $\mathbb{C}[X, Y]$ é do tipo $(X - a, Y - b)$ com $a, b \in \mathbb{C}$. Os ideais maximais de $R = \mathbb{C}[X, Y]/I$ são do tipo $(X - a, Y - b)/I$ com $a, b \in \mathbb{C}$ tais que $I \subseteq (X - a, Y - b)$. A condição $I \subseteq (X - a, Y - b)$ é equivalente a $X^2 - Y^2 - 1 \in (X - a, Y - b)$ ou seja existem $f, h \in \mathbb{C}[X, Y]$ tais que $X^2 - Y^2 - 1 = (X - a)f + (Y - b)h$. Substituindo $X = a$ e $Y = b$ obtemos $a^2 - b^2 - 1 = 0$. Por outro lado, se $a, b \in \mathbb{C}$ são tais que $a^2 - b^2 - 1 = 0$ então

   $$\begin{aligned} X^2 - Y^2 - 1 &= (X - a)(X + a) - (Y - b)(Y + b) + a^2 - b^2 - 1 \\ &= (X - a)(X + a) - (Y - b)(Y + b) \in (X - a, Y - b). \end{aligned}$$

Isso mostra que os ideais maximais de $\mathbb{C}[X,Y]$ contendo I são exatamente os ideais de $\mathbb{C}[X,Y]$ do tipo $(X-a,Y-b)$ com $a^2-b^2-1=0$, logo os ideais de R são exatamente os ideais do tipo $(X-a,Y-b)/I$ com $a^2-b^2-1=0$.

O resultado não vale com $\mathbb{R}$ no lugar de $\mathbb{C}$, por exemplo, indicando com I o ideal de $\mathbb{R}[X,Y]$ gerado por X^2-Y^2-1, o ideal $J=(X,Y^2+1)/I$ de $R=\mathbb{R}[X,Y]/I$ é maximal pois $R/J\cong\mathbb{R}[Y]/(Y^2+1)\cong\mathbb{C}$ é um corpo mas (X,Y^2+1) não é do tipo $(X-a,Y-b)$ com $a,b\in\mathbb{R}$. De fato se fosse $(X,Y^2+1)=(X-a,Y-b)$ poderiamos escrever $Y^2+1=(X-a)f+(Y-b)h$ com $f,h\in\mathbb{R}[X,Y]$ e substituindo $X=a$ e $Y=b$ obteriamos $b^2+1=0$, com $b\in\mathbb{R}$, absurdo.

4. Seja K um corpo. Considere $R:=K[X,Y]/I$ onde $I=(XY-1)$.

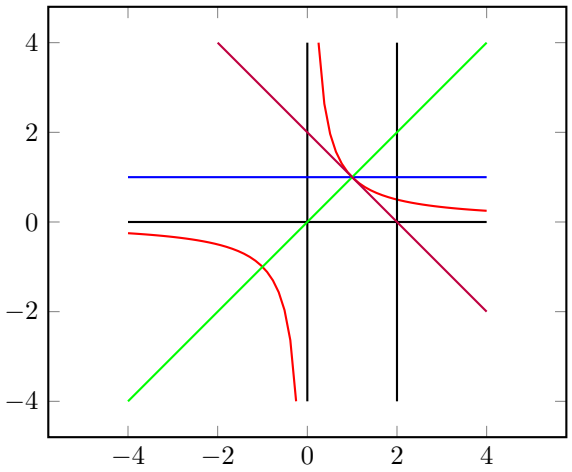
   (a) Mostre que se A é um domínio de ideais principais (PID) e S é um subconjunto de A contendo 1 e multiplicativamente fechado então o localizado $S^{-1}A$ é um domínio de ideais principais (PID). Seja J um ideal de $S^{-1}A$, assim $J=S^{-1}I$ para algum ideal I de R, assim I é principal gerado por um elemento $a\in R$. Deduzimos que

   $$J=S^{-1}I=\{ar/s\ :\ r\in R,\ s\in S\}=(a/1).$$

   (b) Mostre que R é um domínio de ideais principais (PID). [Dica. Observe que R é isomorfo a um localizado de $K[X]$ (qual?).] Observe que $R=K[X,Y]/(XY-1)$ é isomorfo ao localizado $S^{-1}K[X]$ onde $S=\{X^n\ :\ n\in\mathbb{N}\}$ (aqui $0\in\mathbb{N}$). Pelo item anterior R é um PID.

   (c) Deduza que R é um domínio de Dedekind. [Dica. Mostre que um PID tem dimensão no máximo 1.] Pelo item anterior R é um PID, além disso não é um corpo, de fato $X+1$ não é inversível em R: se fosse inversível, poderiamos escrever $1/(X+1)=P(X)/X^n$ para algum $P(X)\in K[X]$, ou seja $X^n=(X+1)P(X)$, e isso contradiz a fatoração única em $K[X]$ (que é UFD), pois X e $X+1$ são irredutíveis. Se um anel A é PID e não é corpo então $\dim(A)=1$. De fato, se $I=(a)$ é um ideal primo não nulo, então considere $B:=A/(a)$, mostraremos que é um corpo. Os ideais de B são do tipo $(x)/(a)$ com $(x)\supseteq(a)$, assim existe $y\in R$ tal que $xy=a$, logo $xy\in(a)$, e como (a) é ideal primo, $x\in(a)$ ou $y\in(a)$. Se $x\in(a)$ então $x=ar$ com $r\in A$, segue que $a=xy=ary$ logo $a(1-ry)=0$ e como A é domínio e $a\neq0$, segue que $ry=1$, logo y é inversível, logo $(x)=(xy)=(a)$ e $(x)/(a)=(a)/(a)$ é o ideal nulo. Se $y\in(a)$ então $y=as$ com $s\in A$, segue que $a=xy=asx$ logo $a(1-sx)=0$ e como A é domínio e $a\neq0$, segue que $sx=1$, logo x é inversível, logo $(x)/(a)=A/(a)$. Isso mostra que os únicos ideais de $A/(a)$ são $(a)/(a)$ e $A/(a)$, logo $A/(a)$ é corpo, ou seja (a) é um ideal maximal de A.

(d) Sejam $x := X + I$, $y := Y + I$, elementos de R. Fatore os ideais principais $(x-2)$, $(y-1)$, $(x-y)$, $(x+y-2)$ de R como produtos de ideais primos de R. [Dica. Faça um desenho das curvas envolvidas.]



Os primos das fatorações correspondem às interseções com a hipérbola, assim temos

- $(x-2) = (x-2, y-1/2)$ e $(y-1) = (x-1, y-1)$ são primos.
- $(x-y) = (x-1, y-1)(x+1, y+1)$.
- $(x+y-2) = (x-1, y-1)^2$.

5. Seja K uma extensão finita de $\mathbb{Q}$, ou seja $\mathbb{Q}$ é um subcorpo de K e a dimensão $|K : \mathbb{Q}| = \dim_{\mathbb{Q}}(K)$ é finita. Seja R o anel dos inteiros de K, ou seja R é o conjunto dos elementos de K que são raízes de polinômios mônicos de $\mathbb{Z}[X]$. Seja I um ideal não nulo de R. Mostre que R/I é um anel finito.

   [Dica. Lembre-se que R é finitamente gerado como $\mathbb{Z}$-módulo.]

   É verdade que se D é um domínio de Dedekind qualquer e $\{0\} \neq I \trianglelefteq D$ então D/I é sempre um anel finito?

   Primeira pergunta. Seja I um ideal não nulo de R e seja $a \in I$ diferente de zero. Seja $P(X) \in \mathbb{Z}[X]$ o polinômio minimal de a sobre $\mathbb{Q}$, então $P(X)$ é mônico e tem coeficientes inteiros, logo $n := P(0) \in \mathbb{Z} \cap I$ e $n \neq 0$. Como $0 \neq -n \in \mathbb{Z} \cap I$, podemos supor $n > 0$. Seja $\{r_1, \ldots, r_m\}$ um conjunto gerador de R como $\mathbb{Z}$-módulo. Temos então que $nr_i \in I$ para todo $i = 1, \ldots, m$, sendo $n \in I$. Isso implica que $|R/I| \leq n^m$.

   Segunda pergunta. Não, por exemplo $\mathbb{Q}[X]/(X) \cong \mathbb{Q}$ é infinito.