Exercise Sheet 7
Algebraic Number Theory

November 26, 2025

Exercise 1. Let A be a Dedekind ring with field of fractions K. Let $L = K(\theta)$ with $[L : K] = d$ and let $a \in A$. Prove that

$$\mathrm{disc}_{L/K}(1, \theta, ..., \theta^{d-1}) = \mathrm{disc}_{L/K}(1, (\theta - a), ..., (\theta - a)^{d-1}).$$

Solution. If we assume that L/K is separable, then the proof is very easy using Exercise 1, Sheet 6. In fact by writing $\{\sigma_1, \ldots, \sigma_d\} = \mathrm{Hom}_K(L, \bar{K})$, for some algebraic closure $\bar{K}$ of K, then we would have

$$\begin{aligned}\mathrm{disc}_{L/K}(1, (\theta - a), \ldots, (\theta - a)^{d-1}) &= \prod_{1 \le i < j \le d} (\sigma_i(\theta - a) - \sigma_j(\theta - a))^2 \\ &= \prod_{1 \le i < j \le d} (\sigma_i(\theta) - \sigma_j(\theta))^2 = \mathrm{disc}_{L/K}(1, \theta, \ldots, \theta^{d-1}).\end{aligned}$$

Without assuming that L/K is separable it is a bit more annoying. We present here the case $d = 3$ for two reasons. The main one is that it contains already the ideas to solve the general case and it easier to follow, the second one is because it is tedious to write one the case for general d for notation reasons.

$$\begin{aligned}\mathrm{disc}_{L/K}(1, \theta - a, (\theta - a)^2) &= \left| \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\theta - a) & \mathrm{tr}((\theta - a)^2) \\ \mathrm{tr}(\theta - a) & \mathrm{tr}((\theta - a)^2) & \mathrm{tr}((\theta - a)^3) \\ \mathrm{tr}((\theta - a)^2) & \mathrm{tr}((\theta - a)^3) & \mathrm{tr}((\theta - a)^4) \end{pmatrix} \right| \\ &= \left| \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\theta - a) & \mathrm{tr}(\theta^2 - 2a\theta + a^2) \\ \mathrm{tr}(\theta - a) & \mathrm{tr}(\theta^2 - 2a\theta + a^2) & \mathrm{tr}(\theta^3 - 3a\theta^2 + 3a^2\theta - a^3) \\ \mathrm{tr}(\theta^2 - 2a\theta + a^2) & \mathrm{tr}(\theta^3 - 3a\theta^2 + 3a^2\theta - a^3) & \mathrm{tr}(\theta^4 - 4a\theta^3 + 6a^2\theta^2 - 4a^3\theta + a^4) \end{pmatrix} \right|.\end{aligned}$$

We use Gauss reduction algorithm on both rows and columns as follows: we multiply on the left by

$$\begin{pmatrix} 1 & & \\ a & 1 & \\ a^2 & 2a & 1 \end{pmatrix}$$

and on the right by

$$\begin{pmatrix} 1 & a & a^2 \\ & 1 & 2a \\ & & 1 \end{pmatrix}.$$

Hence we get

$$\begin{aligned}&\mathrm{disc}_{L/K}(1, \theta - a, (\theta - a)^2) = \\ &\left| \begin{pmatrix} 1 & & \\ a & 1 & \\ a^2 & 2a & 1 \end{pmatrix} \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\theta - a) & \mathrm{tr}((\theta - a)^2) \\ \mathrm{tr}(\theta - a) & \mathrm{tr}((\theta - a)^2) & \mathrm{tr}((\theta - a)^3) \\ \mathrm{tr}((\theta - a)^2) & \mathrm{tr}((\theta - a)^3) & \mathrm{tr}((\theta - a)^4) \end{pmatrix} \begin{pmatrix} 1 & a & a^2 \\ & 1 & 2a \\ & & 1 \end{pmatrix} \right| = \\ &\left| \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\theta) & \mathrm{tr}(\theta^2) \\ \mathrm{tr}(\theta) & \mathrm{tr}(\theta^2) & \mathrm{tr}(\theta^3) \\ \mathrm{tr}(\theta^2) & \mathrm{tr}(\theta^3) & \mathrm{tr}(\theta^4) \end{pmatrix} \right| = \mathrm{disc}_{L/K}(1, \theta, \theta^2)\end{aligned}$$

For the general d use the binomial expansion and the same strategy as before (row and column reduction).

Exercise 2. The goal of this exercise is to show that the ring of integers of $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ is not monogeneous, i.e. $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. Let $\alpha \in O_K$ and Let $f \in \mathbb{Z}[X]$ be its minimal polynomial. For any $g \in \mathbb{Z}[X]$ we denote by $\overline{g}$ the image of g under the unique ring morphism $\mathbb{Z}[X] \to \mathbb{F}_3[X]$ which maps $X \mapsto X$ and $\mathbb{Z} \ni a \mapsto a \,(\mathrm{mod}\, 3)$.

1. Let $g \in \mathbb{Z}[X]$. Show that 3 divides $g(\alpha)$ in $\mathbb{Z}[\alpha]$ if and only if $\overline{f}$ divides $\overline{g}$ in $\mathbb{F}_3[X]$.

2. We now assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Consider the following four elements of $\mathcal{O}_K$

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$$
$$\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$$
$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$$
$$\alpha_4 = (1-\sqrt{7})(1-\sqrt{10}).$$

   Show that all products $\alpha_i\alpha_j$ $(i \neq j)$ are divisible by 3 in $\mathbb{Z}[\alpha]$, but 3 does not divide any power of α_i.

   Hint: Show that $\alpha_i^n/3$ is not in $\mathcal{O}_K$ by considering its trace: Show that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$$

   and show that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n)$ is congruent modulo 3 (in $\mathbb{Z}[\alpha]$) to

$$(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n = 4^n.$$

3. Let $\alpha_i = f_i(\alpha)$, $f_i \in \mathbb{Z}[X]$ for all $i = 1, 2, 3, 4$. Show that $\overline{f} \mid \overline{f_i f_j}$ $(i \neq j)$ in $\mathbb{F}_3[X]$ but $\overline{f} \nmid \overline{f_i}^n$. Conclude that for all i it exists an irreducible factor of $\overline{f}$ (in $\mathbb{F}_3$) that does not divide $\overline{f_i}$ but divides all $\overline{f_j}$, $i \neq j$.

4. Part c) shows that $\overline{f}$ has at least four irreducible factors in $\mathbb{F}_3$. Argue why this contradicts the fact that f is of degree at most 4.

5. Conclude that O_K is not monogeneous.

Solution. 1. Consider the morphism

$$\Phi\colon \mathbb{Z}[X] \to \mathbb{F}_3[X] \to \mathbb{F}_3[X]/(\bar{f}).$$

   Since $f \in \ker(\Phi)$ we get also the morphism

$$\bar{\Phi}\colon \mathbb{Z}[X]/(f) \to \mathbb{F}_3[X]/(\bar{f}),$$

   so that $\bar{\Phi} \circ (\mathbb{Z}[X] \to \mathbb{Z}[X]/(f)) = \Phi$. Explicitely, $\bar{\Phi}([\sum_k a_k X^k]) = [\sum_k a_k \,(\mathrm{mod}\, 3) X^k]$. Recall that $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(f)$, so that there is a morphism

$$\Psi\colon \mathbb{Z}[\alpha] \to \mathbb{F}_3[X]/(\bar{f}) \text{ so that } \Psi \circ (\mathbb{Z}[X] \overset{ev_\alpha}{\to} \mathbb{Z}[\alpha]) = \Phi.$$

   Explicitely, $\Psi(\sum_k a_k \alpha^k) = [\sum_k a_k \,(\mathrm{mod}\, 3) X^k] = \sum_k (a_k \,(\mathrm{mod}\, 3))[X]^k$ Suppose $3|g(\alpha)$ in $\mathbb{Z}[\alpha]$, then $\Psi(3)|\Psi(g(\alpha))$ in $\mathbb{F}_3[X]/(\bar{f})$, but $\Psi(3) = 0$, hence $\Psi(g(\alpha)) = 0$. We deduce that $\Phi(g) = 0$, that is $\bar{f}|\bar{g}$. On the other hand, suppose $\bar{f}|\bar{g}$, then $\Phi(g) = 0$. Write $g(\alpha) = \sum_{k=0}^{\deg(f)-1} a_k \alpha^k$, then $0 = \Psi(g(\alpha)) = \sum_{k=0}^{\deg f - 1} (a_k \,(\mathrm{mod}\, 3))[X]^k$. Since $\{1, \ldots, [X]^{\deg(f)-1}\}$ is linearly independent over $\mathbb{F}_3[X]/(\bar{f})$ we deduce that $a_k \equiv 0 \,(\mathrm{mod}\, 3)$ and so $g(\alpha) \in 3\mathbb{Z}[\alpha]$.

2. We have

$$\alpha_1\alpha_2 = -9(1+\sqrt{7})^2, \alpha_1\alpha_3 = -6(1+\sqrt{10})^2, \alpha_1\alpha_4 = (-6)(-9) \in 3\mathbb{Z}[\alpha].$$

   The remaining cases are similar.

Notice that $\mathrm{Hom}_{\mathbb{Q}}(K,\overline{\mathbb{Q}})$ has four elements $\{id,\sigma_7,\sigma_{10},\sigma_7\sigma_{10}\}$, where $\sigma_7(\sqrt{7})=-\sqrt{7}$ and fixes $\sqrt{10}$, whereas $\sigma_{10}(\sqrt{10})=-\sqrt{10}$ and fixes $\sqrt{7}$. In particular, for each $1\leq i,j\leq 4$ there is a unique σ so that $\sigma(\alpha_i)=\alpha_j$. We deduce

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i^n)=\sum_{\sigma\in\mathrm{Hom}_{\mathbb{Q}}(K,\overline{\mathbb{Q}})}\sigma(\alpha_i^n)=\sum_{\sigma\in\mathrm{Hom}_{\mathbb{Q}}(K,\overline{\mathbb{Q}})}\sigma(\alpha_i)^n=(\alpha_1^n+\cdots+\alpha_4^n).$$

Expand now

$$\begin{aligned}(\alpha_1+\cdots+\alpha_4)^n&=\sum_{k_1=0}^{n}\sum_{k_2=0}^{n-k_1}\sum_{k_3=0}^{n-k_1-k_2}\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3}\alpha_1^{k_1}\alpha_2^{k_2}\alpha_3^{k_3}\alpha_4^{n-k_1-k_2-k_3}\\&\equiv\alpha_1^n+\alpha_2^n+\alpha_3^n+\alpha_4^n\,(\mathrm{mod}\,3\mathbb{Z}[\alpha]).\end{aligned}$$

We see that $\alpha_1+\cdots+\alpha_4=4$ and so $1\equiv\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i^n)\equiv 3\,(\mathrm{mod}\,\mathbb{Z}[\alpha])$, since both lies in $\mathbb{Z}$ we see that $1\equiv\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i^n)\,(\mathrm{mod}\,3)$. On the other hand, if $\alpha_i^n\in 3O_K$, then by linearity of the trace $\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i^n)\in 3\mathbb{Z}$, but this is readily false by what we proved before.

3. We apply the first point to see that $\bar{f}|\overline{f_if_j}$ whenever $i\neq j$ and $\bar{f}\nmid\overline{f_i^n}=\overline{f_i}^n$. Since $\mathbb{F}_3[X]$ is a UFD there is a an irreducible factor $P|\bar{f}$ so that $P\nmid\overline{f_i}$. Since $P|\overline{f_if_j}$ $(j\neq i)$ we deduce $P|\overline{f_j}$.

4. We fix $P_1,\ldots,P_4$ monic so that $P_i|\bar{f}$, $P_i\nmid\overline{f}_i$ and $P_i|\overline{f}_j$ for $j\neq i$. Then $P_1,\ldots,P_4$ are pairwise coprime and so $P_1\cdots P_4|\overline{f}$. However $\mathbb{F}_3[X]$ has 3 monic polynomial of degree 1, that is X, $X+1$, $X-1$. That is at least one of the P_i has degree ≥ 2. Hence $\deg(f)\geq 5$.

   On the other hand, $\deg(f)\leq[K:\mathbb{Q}]=4$. In particular, we deduce that there are no such $f_1,\ldots,f_4$ so that $f_i(\alpha)=\alpha_i$ for all $1\leq i\leq 4$.

5. If $O_K=\mathbb{Z}[\alpha]$, then we would be able to find $f_1,\ldots,f_4$ so that $f_i(\alpha)=\alpha_i$ which not possible.

Exercise 3. Let A be a Dedekind ring with field of fractions K. Let L/K be a finite, separable field extension, and let B be the integral closure of A in L. Let $\mathcal{B}$ be a K-basis of L contained in B. Finally, let M be the free A-module generated by $\mathcal{B}$, and let $\iota:M\to B$ be the canonical injection into B.

1. Prove that $\mathcal{B}$ is an A-basis of B if and only if it is an $A_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}}$ for every $\mathfrak{p}\in\mathrm{spec}(A)$.

2. Prove that if A is a principal ideal domain, then

$$\det(\iota)^2\mathfrak{D}_{B/A}=(\mathrm{disc}_{L/K}(\mathcal{B})).\tag{1}$$

   Hint: you can assume the existence of aligned bases for free finitely generated modules over PID. That is, there exist $(b_j)_{1\leq j\leq d}$ a basis of B as A-module and $(a_j)_{1\leq j\leq d}\in A$ so that $(a_jb_j)_{1\leq j\leq d}$ is a basis of M.

3. Show that if A is a principal ideal domain and $\mathfrak{p}\in\mathrm{spec}(A)$, then $\mathcal{B}$ is an $A_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}}$ if and only if $\mathfrak{p}\nmid(\det(\iota))$.

4. We do not assume that A is a PID anymore. Show that if $(\mathrm{disc}_{L/K}(\mathcal{B}))$ is a squarefree ideal, then $\mathcal{B}$ is an A-basis of B.

Solution. In what follows $d=[L:K]$ and $\mathcal{B}=\{b_1,\ldots,b_d\}$.

1. In both implications we just have to show that $\mathcal{B}$ is generating since the linearly independence follows from the fact that $\mathcal{B}$ is K-linearly independent.

   Let $x\in B_{\mathfrak{p}}$. Write $x=\frac{b}{s}$, for $b\in B$ and $s\in A\smallsetminus\{\mathfrak{p}\}$. Let $a_1,\ldots,a_d\in A$ so that $b=a_1b_1+\cdots+a_db_d$, hence $\frac{b}{s}=\frac{a_1}{s}\frac{b_1}{1}+\ldots\frac{a_d}{s}\frac{b_d}{1}$. Hence $\mathcal{B}$ generates $B_{\mathfrak{p}}$ as $A_{\mathfrak{p}}$-vector space.

   Suppose that $\mathcal{B}$ is a $A_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}}$ for each $\mathfrak{p}\in\mathrm{spec}(A)$. Suppose $B\neq M$ and let $b\in B\smallsetminus M$. Consider the proper ideal (since it does not contain 1)

$$\mathfrak{a}=\{x\in A\mid xb\in M\}\subset A,$$

   then $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{m}$. We can write $b=\sum_{i=1}^d\frac{a_i}{s_i}b_i$ for some $a_1,\ldots,a_d\in A$, $s_i\in A\smallsetminus\mathfrak{m}$. But then $s=s_1\cdots s_d$ satisfies $sb=\sum_{i=1}^d\frac{s}{s_i}a_ib_i\in M$ and so $s\in\mathfrak{a}\subset\mathfrak{m}$ which is a contradiction.

2. We follow the hint and fix a basis $(b_j)_{1\le j\le d} \subset B$ and $(a_j)_{1\le j\le d} \subset A$ so that $(a_j b_j)_{1\le j\le d}$ is a basis of M. With respect to these basis we have

$$\iota = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_d \end{pmatrix}.$$

From the class we have $\mathfrak{D}_{B/A} = (\mathrm{disc}_{L/K}(b_1, \dots, b_d))$ and $(\mathrm{disc}_{L/K}(\mathcal{B})) = (\mathrm{disc}_{K/L}(a_1 b_1, \dots, a_d b_d))$. Hence

$$\begin{aligned} \det(\iota)^2 \mathfrak{D}_{B/A} &= (a_1 \dots a_d)^2 (\mathrm{disc}_{K/L}(b_1, \dots, b_d)) \\ &= (\mathrm{disc}_{K/L}(a_1 b_1, \dots, a_d b_d)) = (\mathrm{disc}_{K/L}(\mathcal{B})) \end{aligned}$$

3. Under the given hypothesis on $\mathcal{B}$ we see that $\mathcal{B}$ is an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$ if and only if $\det(\iota)$ is a unit in $A_\mathfrak{p}$, that is, if and only if $\mathfrak{p} \nmid (\det(\iota))$.

4. Suppose $(\mathrm{disc}_{L/K}(\mathcal{B}))$ is a squafree-ideal. Let $\mathfrak{p} \subset A$ be a prime ideal. From (1) we have

$$\det(\iota)^2 \mathfrak{D}_{B/A} A_\mathfrak{p} = \mathrm{disc}_{K/L}(\mathcal{B}) A_\mathfrak{p}.$$

From the class, we also have $\mathfrak{D}_{B/A} A_\mathfrak{p} = \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$. Since $(\mathrm{disc}_{L/K}(\mathcal{B}))$ is a squafree-ideal, we see that $\mathfrak{p}^2 A_\mathfrak{p} \nmid \mathrm{disc}_{K/L}(\mathcal{B}) A_\mathfrak{p}$ and so $\mathfrak{p} A_\mathfrak{p} \nmid \det(\iota) A_\mathfrak{p}$. This is true for every $\mathfrak{p}$ prime ideal and so $(\det(\iota)) = B$, that is, $\det(\iota)$ a unit in A. Hence, $\iota \colon M \to B$ is an isomorphism of A-modules.

Exercise 4. Let A be a Dedekind ring, K its field of fractions, and $\overline{K}$ be an algebraic closure of K. Let $\alpha \in \overline{K}$ be integral over A, $P_\alpha \in A[X]$ be its minimal polynomial, and set $B := A[\alpha]$. Moreover, let $\mathfrak{p}$ be a prime ideal of A, and denote by $\overline{P_\alpha} \in (A/\mathfrak{p})[X]$ the image of P_α under the natural projection $A[X] \to (A/\mathfrak{p})[X]$.

The aim of this exercise is to show that there is bijective correspondence between the ideals of B containing $\mathfrak{p}$ and the monic factors of $\overline{P_\alpha}$.

1. Let $Q \in (A/\mathfrak{p})[X]$ be a divisor of $\overline{P_\alpha}$. Choose $F \in A[X]$ such that $\overline{F} = Q$, and define

$$I(Q) := \mathfrak{p}B + F(\alpha)B \subset B.$$

Prove that $I(Q)$ is well-defined, i.e. that it does not depend on the specific choice of F.

2. Show that the evaluation map $e_\alpha : A[X] \to B$, $f \mapsto f(\alpha)$ induces an isomorphism

$$B \cong A[X]/(P_\alpha),$$

that is, show that if $f \in A[X]$ is so that $f(\alpha) = 0$, then $P_\alpha | f$ already in $A[X]$.

Hint: Write $f = P_\alpha \cdot h$ for some $h \in K[X]$. To show that $h \in A[X]$ first show that $h \in A_\mathfrak{q}[X]$ for any prime ideal $\mathfrak{q} \in \mathrm{spec}(A)$. Then try to show $A = \bigcap_{\mathfrak{q} \in \mathrm{spec}(A)} A_\mathfrak{q}$.

3. Consider the following surjective maps

$$B/\mathfrak{p}B \leftarrow B \xleftarrow{e_\alpha} A[X] \to (A/\mathfrak{p})[X] \to (A/\mathfrak{p})[X]/(\overline{P_\alpha}),$$

and prove that we have a ring isomorphism

$$B/\mathfrak{p}B \cong (A/\mathfrak{p})[X]/(\overline{P_\alpha}).$$

Furthermore, verify that if $Q \in (A/\mathfrak{p})[X]$ is a divisor of $\overline{P_\alpha}$, the ideal $(Q)/(\overline{P_\alpha})$ corresponds to the ideal $I(Q)/\mathfrak{p}B$ under this isomorphism.

4. Conclude that the map $Q \mapsto I(Q)$ gives a bijection between the monic factors of $\overline{P_\alpha}$ and the ideals in B containing $\mathfrak{p}$ in such a way that $Q' \mid Q$ if and only if $I(Q) \subset I(Q')$.

Solution. 1. Suppose $F_1, F_2 \in A[X]$ are so that $\overline{F}_1 = \overline{F_2} = Q \in (A/\mathfrak{p})[X]$. Then $(F_1 - F_2) \in (\mathfrak{p}A)[X]$ and so $F_1 - F_2(\alpha) \in \mathfrak{p}B$. That is,

$$\mathfrak{p}B + F_1(\alpha)B = \mathfrak{p}B + (F_2(\alpha) - F_1(\alpha))B + F_1(\alpha)B = \mathfrak{p}B + F_2(\alpha)B.$$

2. Let $f \in A[X]$ be so that $f(\alpha) = 0$. Since P_α is the minimal polynomial of α, we see that there is a $h \in K[X]$ so that $f = P_\alpha \cdot h$. Let $\mathfrak{p}$ be a prime ideal of A. Then, $A_\mathfrak{p}$ is a PID and it is integrally closed in its fraction field $K = \mathrm{Frac}(A_\mathfrak{q})$. Since P_α is monic, we see that $f = P_\alpha \cdot h'$ for some $h' \in A_\mathfrak{p}[X]$. Of course, $h = h'$ and so we see that $h \in A_\mathfrak{p}[X]$. Since $\mathfrak{p}$ was arbitrary we see that $h \in \bigcap_\mathfrak{p} A_\mathfrak{p}[X] = A[X]$. For the last equality see solutions of Exercise Sheet 6, Exercise 3.

   The map e_α is surjective by assumption.

3. We have a surjective homomorphism

$$A[X] \to B/\mathfrak{p}B; f \mapsto f(\alpha) + \mathfrak{p}B$$

   Its Kernel is the ideal in generated by $\mathfrak{p}$ and P_α. That is we have an isomorphism

$$A[X]/(\mathfrak{p}, P_\alpha) \simeq B/\mathfrak{p}B.$$

   By isomorphism theorems we also have

$$A[X]/(\mathfrak{p}, P_\alpha) \simeq (A[X]/\mathfrak{p})/((\mathfrak{p}, P_\alpha)/\mathfrak{p}) \simeq (A/\mathfrak{p})[X]/(\overline{P}_\alpha).$$

   Take $Q|\overline{P}_\alpha$ and let $F \in A[X]$ so that $\overline{F} = Q$. Then the last row identifies $(Q)/(\overline{P}_\alpha)$ with $(FA[X] + \mathfrak{p}A[X])/(\mathfrak{p}, P_\alpha)$. The latter is mapped by the second row to $(F(\alpha)B + \mathfrak{p}B)/\mathfrak{p}B$.

4. It remains to show that $Q|Q'$ if and only if $I(Q) \subset I(Q')$: let $Q, Q'|\overline{P}_\alpha$ and let $F, F' \in A[X]$ be so that $\overline{F} = Q$, $\overline{F'} = Q'$. Then we have

$$\begin{aligned} Q|Q' &\Leftrightarrow (Q)/(\overline{P_\alpha}) \supset (Q')/(\overline{P}_\alpha) \\ &\Leftrightarrow (F(\alpha)B + \mathfrak{p}B)/\mathfrak{p}B \supset (F'(\alpha)B + \mathfrak{p}B)/\mathfrak{p}B \\ &\Leftrightarrow F(\alpha)B + \mathfrak{p}B \supset F'(\alpha)B + \mathfrak{p}B \end{aligned}$$