1. Resultants

- *Show that if α is a root of a monic polynomial in $\mathbb{Z}[x]$ and $\lambda \in \mathbb{Z}$ then $\lambda\alpha$ is a root of a monic polynomial in $\mathbb{Z}[x]$.*

2. Algebraic Integers

- ***Gauss's Lemma.***
  1. *Show that if $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ and $g(x)$ and $h(x)$ are monic polynomials in $\mathbb{Q}[x]$ and $f(x) = g(x)\,h(x)$ then $g(x)$ and $h(x)$ belong to $\mathbb{Z}[x]$.*
  2. *Apply Gauss's Lemma to show that the (monic) minimal polynomial of an algebraic integer has integer coefficients.*

- ***Vandermonde Determinants.***

  Show that if

$$V = \begin{bmatrix} 1 & v_1 & v_1^2 & & v_1^{n-1} \\ 1 & v_2 & v_2^2 & & v_2^{n-1} \\ 1 & v_3 & v_3^2 & & v_3^{n-1} \\ & & & \ddots & \\ 1 & v_n & v_n^2 & & v_n^{n-1} \end{bmatrix}$$

  then $\det V = \prod_{j<k}(v_k - v_j)$.

- *Let $\alpha,\, \beta \in \mathcal{O}$ with $\mathcal{K} = \mathbb{Q}(\alpha)$ and let $\omega = \{\,\omega_1,\, \ldots,\, \omega_n\,\}$ be a $\mathbb{Z}$-module basis for $\mathbb{Z}[\alpha, \beta]$. Then there exists a matrix $T_\omega \in \mathbb{Q}^{n\times n}$, in lower-triangular form and with positive diagonal entries, such that $\omega_j = \sum_{k=1}^{j} (T_\omega)_{j,k}\, \alpha^{k-1}$ for $j = 1,\, \ldots,\, n$. Note that $T_\omega^{-1} \in \mathbb{Z}^{n\times n}$, by the definition of ω.*

  Prove the following.

  1. *For $k = 1,\, \ldots,\, n$ there exists a positive integer d_k such that $(T_\omega)_{kk} = 1/d_k$, and in particular $d_1 = 1$.*

     (Use the fact that α^{k-1} can be expressed uniquely as a $\mathbb{Z}$-linear combination of $\omega_1,\, \ldots,\, \omega_n$.)
  2. *d_k is a multiple of d_{k-1} for $k = 2,\, \ldots,\, n$.*

     (Use the fact that if $\lambda_k d_k + \mu_k d_{k-1} = \gcd(d_k, d_{k-1})$ for integers λ_k and μ_k then $\lambda_k \alpha\omega_{k-1} + \mu_k \omega_k$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of $\omega_1,\, \ldots,\, \omega_n$.)
  3. *$d_k\omega_k \in \mathbb{Z}[\alpha]$ for $k = 1,\, \ldots,\, n$.*

     (Use the fact that $\alpha\omega_k$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of $\omega_1,\, \ldots,\, \omega_n$.)

3. Computing Integral Bases Efficiently

- *Let $\mathcal{A}$ be an order of $\mathcal{K}$ and let $\{\,\omega_1,\,\ldots,\,\omega_n\,\}$ be a $\mathbb{Z}$-basis for $\mathcal{A}$.*

  1. *Prove that $\mathcal{A} \subseteq \mathcal{O}$, as follows. For an arbitrary element α of $\mathcal{A}$ let*

  $$M_\alpha \;=\; \begin{bmatrix} a_{11} & a_{12} & & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ & & \ddots & \\ a_{n1} & a_{n2} & & a_{nn} \end{bmatrix} \;\in\; \mathbb{Z}^{n\times n}$$

  be given by $\alpha\omega_j = a_{j1}\omega_1 + \cdots + a_{jn}\omega_n$ for $j = 1,\,\ldots,\,n$ and let

  $$\chi_\alpha(x) \;=\; \det(xI - M_\alpha).$$

  Show that $\chi_\alpha(x)$ is a monic polynomial in $\mathbb{Z}[x]$ with $\chi_\alpha(\alpha) = 0$.

  2. *Apply the previous result with $\mathcal{A} = \mathcal{O}$ to show that if $\beta, \gamma \in \mathcal{K}$ and $\beta \neq 0$ and $\beta\gamma^k \in \mathcal{O}$ for all $k \geq 0$ then $\gamma \in \mathcal{O}$.*

- *Let p be prime and define*

$$\begin{aligned} \mathcal{O}_p \;&=\; \{\,\alpha \in \mathcal{O} \mid p\alpha \in \mathcal{A}\,\}, \\ \mathcal{R}_p \;&=\; \{\,\beta \in \mathcal{A} \mid \beta^k \in p\mathcal{A} \text{ for some } k \geq 1\,\}, \\ [\mathcal{R}_p/\mathcal{R}_p] \;&=\; \{\,\gamma \in \mathcal{K} \mid \gamma\mathcal{R}_p \subseteq \mathcal{R}_p\,\}. \end{aligned}$$

For $\theta \in \mathcal{K}$ let μ_θ denote the minimal polynomial of θ over $\mathbb{Q}$. Prove the following.

1. $\gamma\mathcal{R}_p \subseteq \mathcal{R}_p \implies p,\, p\gamma,\, p\gamma^2,\, \ldots \in \mathcal{A} \implies \gamma \in \mathcal{O}$.
2. $[\mathcal{R}_p/\mathcal{R}_p]$ *is an order of* $\mathcal{K}$.
3. $\mathcal{A} \subseteq [\mathcal{R}_p/\mathcal{R}_p] \subseteq \mathcal{O}_p$.
4. $\alpha^k \in p\mathcal{O}$ *for some* $k \geq 1 \implies \mu_\alpha(x) \mid \mu_{p\beta}(x^k)$ *with* $p\beta = \alpha^k$
   $\implies \mu_\alpha(x) \equiv x^m \pmod{p}$ *for some* $m \geq 1$.
5. $\mu_\alpha(x) \equiv x^m \pmod{p}$ *for some* $m \geq 1 \implies \alpha^m \in p\mathcal{A}$
   $\implies \alpha^k \in p\mathcal{O}$ *for some* $k \geq 1$.
6. $\mathcal{R}_p = \{\,\alpha \in \mathcal{A} \mid \alpha^k \in p\mathcal{O} \text{ for some } k \geq 1\,\}$.
7. $[\mathcal{R}_p/\mathcal{R}_p] = \{\,\gamma \in \mathcal{O} \mid \gamma\mathcal{R}_p \subseteq \mathcal{A}\,\}$.