Integral Bases

1. Resultants

Suppose f and g are polynomials in one or more variables (including x) with integer coefficients. Say

$$\begin{aligned} f &= A_0\,x^m + A_1\,x^{m-1} + \cdots + A_m, \\ g &= B_0\,x^n + B_1\,x^{n-1} + \cdots + B_n, \end{aligned}$$

with $A_0, \ldots, A_m$ and $B_0, \ldots, B_n$ polynomials not involving x and with $A_0 \neq 0$ and $B_0 \neq 0$. We recursively define the *resultant of f and g with respect to x* as

$$\operatorname{Res}_x(f,g) = \begin{cases} A_0^n & \text{if } m = 0, \\ B_0^m & \text{if } n = 0, \\ (-1)^{mn}\operatorname{Res}_x(g,f) & \text{if } 0 < m < n, \\ (-1)^{mn}\,B_0^{1-n}\operatorname{Res}_x(g,h) & \text{if } 0 < n \le m, \end{cases}$$

with $h = B_0 f - A_0\,x^{m-n} g$ having lower degree in x than f. If you look closely you can see that

$$\operatorname{Res}_x(f,g) = \det \begin{bmatrix} A_0 & \cdots & A_m & 0 & 0 & \cdots & 0 \\ 0 & A_0 & \cdots & A_m & 0 & \cdots & 0 \\ 0 & 0 & A_0 & \cdots & A_m & \cdots & 0 \\ & & & \ddots & & \ddots & \\ 0 & 0 & 0 & \cdots & A_0 & \cdots & A_m \\ B_0 & \cdots & B_n & 0 & 0 & \cdots & 0 \\ 0 & B_0 & \cdots & B_n & 0 & \cdots & 0 \\ 0 & 0 & B_0 & \cdots & B_n & \cdots & 0 \\ & & & \ddots & & \ddots & \\ 0 & 0 & 0 & \cdots & B_0 & \cdots & B_n \end{bmatrix}$$

with $A_0, \ldots, A_m$ appearing in rows 1 through n and $B_0, \ldots, B_n$ appearing in rows $n+1$ through $n+m$. It follows that $\operatorname{Res}_x(f,g)$ is a polynomial in zero or more variables (not including x) with integer coefficients.

When $f(x)$ and $g(x)$ are polynomials in $\mathbb{Z}[x]$ we have

$$\begin{aligned} f(x) &= \lambda\,(x-\alpha_1)\cdots(x-\alpha_m) \\ g(x) &= \mu\,(x-\beta_1)\cdots(x-\beta_n) \end{aligned}$$

with $\alpha_1, \ldots, \alpha_m$, $\beta_1, \ldots, \beta_n$ complex, and the resultant has the charming property that

$$\operatorname{Res}_x\bigl(f(x),g(x)\bigr) = \lambda^n\mu^m\textstyle\prod_{j=1}^m\prod_{k=1}^n(\alpha_j-\beta_k) = \lambda^n\prod_{j=1}^m g(\alpha_j).$$

Even better, if $f(x)$ and $g(x)$ are monic polynomials in $\mathbb{Z}[x]$ then

$$\begin{aligned} \operatorname{Res}_x\bigl(f(x),\operatorname{Res}_y\bigl(g(y),t-xy\bigr)\bigr) &= \operatorname{Res}_x\bigl(f(x),\textstyle\prod_{k=1}^n(t-x\beta_k)\bigr) \\ &= \textstyle\prod_{j=1}^m\prod_{k=1}^n(t-\alpha_j\beta_k) \quad \in \mathbb{Z}[t], \\ \operatorname{Res}_x\bigl(f(x),\operatorname{Res}_y\bigl(g(y),t-x-y\bigr)\bigr) &= \operatorname{Res}_x\bigl(f(x),\textstyle\prod_{k=1}^n(t-x-\beta_k)\bigr) \\ &= \textstyle\prod_{j=1}^m\prod_{k=1}^n(t-\alpha_j-\beta_k) \quad \in \mathbb{Z}[t]. \end{aligned}$$

Consequently, if α and β are roots of monic polynomials in $\mathbb{Z}[x]$ then so are $\alpha\beta$ and $\alpha+\beta$.

Exercise. *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 $\mathbb{Z}[x]$.*

Example. Let $f(x) = x^2 - 2$, $g(y) = y^2 + 5$. Then

$$\begin{aligned} r_y(t,x) &= \operatorname{Res}_y\bigl(g(y),t-x-y\bigr) \\ &= \det\begin{bmatrix} 1 & 0 & 5 \\ -1 & t-x & 0 \\ 0 & -1 & t-x \end{bmatrix} = x^2 - 2tx + t^2 + 5, \end{aligned}$$

$$\begin{aligned} r_{x,y}(t) &= \operatorname{Res}_x\bigl(f(x),r_y(t,x)\bigr) \\ &= \det\begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & -2t & t^2+5 & 0 \\ 0 & 1 & -2t & t^2+5 \end{bmatrix} = t^4 + 6t^2 + 49. \end{aligned}$$

2. Algebraic Integers

An *algebraic integer* is a root of a monic polynomial in $\mathbb{Z}[x]$.

For example, if k is an integer and $\alpha = \frac{1}{2}(1+\sqrt{4k+1})$ then α is a root of $x^2 - x - k$, so α is an algebraic integer.

Exercise: ***Gauss's Lemma.***
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 $\mathbb{Z}[x]$.

Exercise. *Apply Gauss's Lemma to show that the (monic) minimal polynomial of an algebraic integer has integer coefficients.*

The set of algebraic integers belonging to an algebraic number field $\mathcal{K}$ we denote by $\mathcal{O}_\mathcal{K}$ or simply $\mathcal{O}$. From the discussion above it follows that $\mathcal{O}_\mathcal{K}$ is both a ring and a $\mathbb{Z}$-module.

Suppose β is a nonzero algebraic integer with $h(x)$ its minimal polynomial over $\mathbb{Q}$ and m the degree of $h(x)$, and let λ be a positive integer. Then the minimal polynomial of β/λ is $\lambda^{-m}h(\lambda x)$, which will not be in $\mathbb{Z}[x]$ if $\lambda^m > |h(0)|$.

For example, if β is a root of $x^2 - 2x - 4$ then $\beta/2$ is a root of $x^2 - x - 1$, but the minimal polynomial of $\beta/4$ is $x^2 - \frac{1}{2}x - \frac{1}{4}$, so $\beta/4$ is not an algebraic integer.

Exercise: ***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

$$\det V \;=\; \prod\nolimits_{j<k}(v_k - v_j).$$

Let $f(x)$ be an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree n, let α be a root of $f(x)$, and let $\mathcal{O}$ be the set of algebraic integers belonging to $\mathbb{Q}(\alpha)$.

Suppose $\beta \in \mathcal{O}$. Then

$$\mathbb{Z}[\alpha,\beta] \;=\; \sum\nolimits_{1\le j\le n,\,1\le k\le n} \mathbb{Z}\,\alpha^{j-1}\beta^{k-1} \;\subseteq\; \mathcal{O}$$

and the elements $\alpha^{j-1}\beta^{k-1}$, $1 \le j \le n$, $1 \le k \le n$, expressed as vectors over $\mathbb{Q}$, can be reduced over $\mathbb{Z}$ (note!) to give a $\mathbb{Z}$-module basis $\{\,\omega_1,\,\omega_2,\,\ldots,\,\omega_n\,\}$ for $\mathbb{Z}[\alpha,\beta]$. Since $\{\,1,\,\alpha,\,\alpha^2,\,\ldots,\,\alpha^{n-1}\,\}$ is a vector-space basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ there is a matrix $T_\omega \in \mathbb{Q}^{n\times n}$ such that

$$\begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \\ \vdots \\ \omega_n \end{bmatrix} \;=\; T_\omega \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \end{bmatrix}.$$

Note that without loss of generality we may construct $\omega_1, \ldots, \omega_n$ so that T_ω is lower-triangular with positive diagonal entries, and so we do. And since

$$\begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \end{bmatrix} \;=\; T_\omega^{-1} \begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \\ \vdots \\ \omega_n \end{bmatrix}$$

it follows that $T_\omega^{-1} \in \mathbb{Z}^{n\times n}$.

Exercise. *Exploit the fact that T_ω is in lower-triangular form with positive diagonal entries to prove the following.*

- *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 $\omega_1, \ldots, \omega_n$.)
- *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 $\omega_1, \ldots, \omega_n$.)
- *$d_k\omega_k \in \mathbb{Z}[\alpha]$ for $k = 1, \ldots, n$.*
  (Use the fact that $\alpha\omega_k$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of $\omega_1, \ldots, \omega_n$.)

Decomposing $f(x)$ into linear factors as $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ we define

$$\operatorname{tr}\big(h(\alpha)\big) \;=\; h(\alpha_1) + h(\alpha_2) + \cdots + h(\alpha_n)$$

for $h(x) \in \mathbb{Q}[x]$. If $h(\alpha) \in \mathcal{O}$ then

$$\begin{aligned}\operatorname{Res}_x\big(f(x), t-h(x)\big) \;&=\; \big(t-h(\alpha_1)\big)\cdots\big(t-h(\alpha_n)\big)\\ &=\; t^n \,-\, \operatorname{tr}\big(h(\alpha)\big)\,t^{n-1} + \cdots \pm\, h(\alpha_1)\,h(\alpha_2)\cdots h(\alpha_n)\\ &\in\; \mathbb{Z}[t]\end{aligned}$$

and therefore $\operatorname{tr}\big(h(\alpha)\big) \in \mathbb{Z}$.

Now let

$$A \;=\; \begin{bmatrix} 1 & 1 & 1 & & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & & \alpha_n^2 \\ & & & \ddots & \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & & \alpha_n^{n-1} \end{bmatrix}, \quad A^{\mathsf{T}} \;=\; \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & & \alpha_3^{n-1} \\ & & & \ddots & \\ 1 & \alpha_n & \alpha_n^2 & & \alpha_n^{n-1} \end{bmatrix}$$

so that

$$A\,A^{\mathsf{T}} \;=\; \begin{bmatrix} \operatorname{tr}(1) & \operatorname{tr}(\alpha) & \operatorname{tr}(\alpha^2) & & \operatorname{tr}(\alpha^{n-1}) \\ \operatorname{tr}(\alpha) & \operatorname{tr}(\alpha^2) & \operatorname{tr}(\alpha^3) & & \operatorname{tr}(\alpha^n) \\ \operatorname{tr}(\alpha^2) & \operatorname{tr}(\alpha^3) & \operatorname{tr}(\alpha^4) & & \operatorname{tr}(\alpha^{n+1}) \\ & & & \ddots & \\ \operatorname{tr}(\alpha^{n-1}) & \operatorname{tr}(\alpha^n) & \operatorname{tr}(\alpha^{n+1}) & & \operatorname{tr}(\alpha^{2n-2}) \end{bmatrix}$$

and

$$\det A\,A^{\mathsf{T}} \;=\; \prod\nolimits_{j\neq k}(\alpha_j-\alpha_k)^2 \;=\; \operatorname{disc} f \;=\; (-1)^{n(n-1)/2}\operatorname{Res}_x(f(x), f'(x)).$$

Treating $\omega_1 = \omega_1(\alpha), \ldots, \omega_n = \omega_n(\alpha)$ as polynomials in α we will write ω_{jk} for $\omega_j(\alpha_k)$. We define

$$W \;=\; \begin{bmatrix} \omega_{11} & \omega_{12} & \omega_{13} & & \omega_{1n} \\ \omega_{21} & \omega_{22} & \omega_{23} & & \omega_{2n} \\ \omega_{31} & \omega_{32} & \omega_{33} & & \omega_{3n} \\ & & & \ddots & \\ \omega_{n1} & \omega_{n2} & \omega_{n3} & & \omega_{nn} \end{bmatrix}, \quad W^{\mathsf{T}} \;=\; \begin{bmatrix} \omega_{11} & \omega_{21} & \omega_{31} & & \omega_{n1} \\ \omega_{12} & \omega_{22} & \omega_{32} & & \omega_{n2} \\ \omega_{13} & \omega_{23} & \omega_{33} & & \omega_{n3} \\ & & & \ddots & \\ \omega_{1n} & \omega_{2n} & \omega_{3n} & & \omega_{nn} \end{bmatrix}$$

so that

$$W\,W^{\mathsf{T}} \;=\; \begin{bmatrix} \operatorname{tr}(\omega_1\,\omega_1) & \operatorname{tr}(\omega_1\,\omega_2) & \operatorname{tr}(\omega_1\,\omega_3) & & \operatorname{tr}(\omega_1\,\omega_n) \\ \operatorname{tr}(\omega_2\,\omega_1) & \operatorname{tr}(\omega_2\,\omega_2) & \operatorname{tr}(\omega_2\,\omega_3) & & \operatorname{tr}(\omega_2\,\omega_n) \\ \operatorname{tr}(\omega_3\,\omega_1) & \operatorname{tr}(\omega_3\,\omega_2) & \operatorname{tr}(\omega_3\,\omega_3) & & \operatorname{tr}(\omega_3\,\omega_n) \\ & & & \ddots & \\ \operatorname{tr}(\omega_n\,\omega_1) & \operatorname{tr}(\omega_n\,\omega_2) & \operatorname{tr}(\omega_n\,\omega_3) & & \operatorname{tr}(\omega_n\,\omega_n) \end{bmatrix} \;\in\; \mathbb{Z}^{n\times n}$$

and hence $\det W\,W^{\mathsf{T}} \in \mathbb{Z}$.

On the other hand, with $d_\omega = d_1\cdots d_n$ we have

$$\begin{aligned} W \;&=\; T_\omega A,\\ \det W\,W^{\mathsf{T}} \;=\; \det(T_\omega A\,A^{\mathsf{T}}T_\omega^{\mathsf{T}}) \;&=\; (\det T_\omega)^2(\det A)^2 \;=\; d_\omega^{-2}\operatorname{disc} f,\\ \operatorname{disc} f \;&=\; d_\omega^2 \det W\,W^{\mathsf{T}},\\ T_\omega \;=\; \det T_\omega\,(T_\omega^{-1})^* \;&=\; \frac{1}{d_\omega}\,(T_\omega^{-1})^* \;\in\; \frac{1}{d_\omega}\,\mathbb{Z}^{n\times n}. \end{aligned}$$

Proposition. *If d^2 is the largest square dividing* $\operatorname{disc} f$ *then*

$$\mathbb{Z}[\alpha] \;\subseteq\; \mathcal{O} \;\subseteq\; \frac{1}{d}\,\mathbb{Z}[\alpha].$$

Example. Let $f(x) = x^2 - 14x + 4$. Then $\operatorname{disc} f = 180 = 2^2 \cdot 3^2 \cdot 5$, so that $d = 6$. Among the 35 distinct nonzero representatives of $\frac{1}{d}\mathbb{Z}[\alpha]$ modulo $\mathbb{Z}[\alpha]$ there are five algebraic integers.

$\omega(\alpha)$	$\operatorname{Res}_x\big(f(x), \omega(x), t - x\big)$
$\frac{1}{2}\,\alpha$	$t^2 - 7t + 1$
$\frac{1}{3} + \frac{1}{6}\,\alpha$	$t^2 - 3t + 1$
$\frac{1}{3} + \frac{2}{3}\,\alpha$	$t^2 - 10t + 5$
$\frac{2}{3} + \frac{1}{3}\,\alpha$	$t^2 - 6t + 4$
$\frac{2}{3} + \frac{5}{6}\,\alpha$	$t^2 - 13t + 11$

Row-reduction to lower-triangular form over $\mathbb{Z}$ gives

$$\begin{bmatrix} 1 & \cdot \\ \cdot & 1 \\ \cdot & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{6} \\ \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{5}{6} \end{bmatrix} \longrightarrow \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ 1 & \cdot \\ \frac{1}{3} & \frac{1}{6} \end{bmatrix}$$

and it follows that $\left\{\, 1,\ \frac{1}{3} + \frac{1}{6}\alpha \,\right\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$.

Example. Let $f(x) = x^3 - 7x^2 - x - 1$. Then $\operatorname{disc} f = -1472 = -2^6 \cdot 23$, so that $d = 2^3 = 8$. Among the 511 distinct nonzero representatives of $\frac{1}{d}\mathbb{Z}[\alpha]$ modulo $\mathbb{Z}[\alpha]$ there are seven algebraic integers.

$\omega(\alpha)$	$\operatorname{Res}_x\big(f(x), \omega(x), t - x\big)$
$\frac{1}{2}\alpha + \frac{1}{2}\alpha^2$	$t^3 - 29t^2 - 6t - 1$
$\frac{1}{4} + \frac{3}{4}\alpha^2$	$t^3 - 39t^2 + 12t - 1$
$\frac{1}{4} + \frac{1}{2}\alpha + \frac{1}{4}\alpha^2$	$t^3 - 17t^2 + 6t - 1$
$\frac{1}{2} + \frac{1}{2}\alpha^2$	$t^3 - 27t^2 + 23t - 5$
$\frac{1}{2} + \frac{1}{2}\alpha$	$t^3 - 5t^2 + 4t - 1$
$\frac{3}{4} + \frac{1}{4}\alpha^2$	$t^3 - 15t^2 + 20t - 7$
$\frac{3}{4} + \frac{1}{2}\alpha + \frac{3}{4}\alpha^2$	$t^3 - 44t^2 + 53t - 17$

Row-reduction to lower-triangular form over $\mathbb{Z}$ gives

$$\begin{bmatrix} 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \\ \cdot & \cdot & 1 \\ \cdot & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{4} & \cdot & \frac{3}{4} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & \cdot & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \cdot \\ \frac{3}{4} & \cdot & \frac{1}{4} \\ \frac{3}{4} & \frac{1}{2} & \frac{3}{4} \end{bmatrix} \longrightarrow \begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot \\ \frac{1}{2} & \frac{1}{2} & \cdot \\ \frac{3}{4} & \cdot & \frac{1}{4} \end{bmatrix}$$

and it follows that $\left\{\, 1,\ \frac{1}{2} + \frac{1}{2}\alpha,\ \frac{3}{4} + \frac{1}{4}\alpha^2 \,\right\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$.

3. Computing Integral Bases Efficiently

Often we need to work with the ring of integers of an algebraic number field and so we need an efficient way to find an *integral basis* for the field, *i.e.*, a $\mathbb{Z}$-module basis for its ring of integers. (It is clear that the method sketched in the examples in the previous section is *not* efficient.)

Let $\mathcal{K}$ be an algebraic number field of degree n with ring of integers $\mathcal{O}$.

An *order* of $\mathcal{K}$ is a subring of $\mathcal{K}$ that contains 1 and is also an n-dimensional $\mathbb{Z}$-module. Note that if $\mathcal{K} = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}$ then $\mathbb{Z}[\alpha]$ is an order of $\mathcal{K}$, as is $\mathcal{O}$ itself.

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

Exercises.

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

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

Exercises. *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. $\mathcal{R}_p = \{\,\alpha \in \mathcal{A} \mid \alpha^k \in p\mathcal{O}$ *for some* $k \geq 1\,\}$.
7. $[\mathcal{R}_p/\mathcal{R}_p] = \{\,\gamma \in \mathcal{O} \mid \gamma\mathcal{R}_p \subseteq \mathcal{A}\,\}$.

Proposition. *If $\mathcal{A} \neq \mathcal{O}_p$ then $\mathcal{A} \neq [\mathcal{R}_p/\mathcal{R}_p]$.*

Proof. There exists $m \geq 1$ such that $\mathcal{R}_p^m \subseteq p\mathcal{A}$.

Choose $\gamma \in \mathcal{O}_p \setminus \mathcal{A}$, and while $\gamma\mathcal{R}_p \not\subseteq \mathcal{A}$ replace $\gamma \leftarrow \gamma\alpha \in \gamma\mathcal{R}_p \setminus \mathcal{A}$.

It follows that after m such replacements we would have $\gamma \in \mathcal{A}$.

Therefore, after at most $m - 1$ replacements we will have $\gamma\mathcal{R}_p \subseteq \mathcal{A}$, but with $\gamma \notin \mathcal{A}$, so that $[\mathcal{R}_p/\mathcal{R}_p] \neq \mathcal{A}$. □

Computing $\mathcal{R}_p$.

Let $q = p^{\lceil \log_p n \rceil}$. Then $q \geq n$ and, for $\alpha \in \mathcal{A}$,

$$\alpha^k \in p\mathcal{A} \text{ for some } k \geq 1 \iff \alpha^n \in p\mathcal{A} \iff \alpha^q \in p\mathcal{A}.$$

Take

$$\alpha \;=\; x_1\omega_1 + \cdots + x_n\omega_n \;\in\; \mathcal{A}.$$

Then

$$\begin{aligned} \alpha^p &\equiv x_1^p\omega_1^p + \cdots + x_n^p\omega_n^p \\ &\equiv x_1\omega_1^p + \cdots + x_n\omega_n^p \pmod{p\mathcal{A}} \end{aligned}$$

and so

$$\alpha^q \;\equiv\; x_1\omega_1^q + \cdots + x_n\omega_n^q \pmod{p\mathcal{A}}.$$

Define the matrix T by

$$\omega_k^q \;=\; \sum T_{jk}\,\omega_j.$$

Then

$$\alpha \in \mathcal{R}_p \iff \alpha^q \in p\mathcal{A} \iff \sum T_{jk}x_k \equiv 0 \pmod{p} \text{ for } j = 1, \ldots, n.$$

Solving this system of congruences gives $\mathcal{R}_p$.

Computing $\mathcal{T}_p$.

The computation of $\mathcal{R}_p$ becomes burdensome when p is large. Instead, let

$$\mathcal{T}_p \;=\; \{\, \alpha \in \mathcal{A} \mid \mathrm{tr}(\alpha\beta) \in p\mathbb{Z} \text{ for all } \beta \in \mathcal{A} \,\}.$$

For $i = 1, \ldots, n$ let the matrix W_i express the action of ω_i on $\omega_1, \ldots, \omega_n$, *i.e.*,

$$\omega_i\omega_j \;=\; \sum (W_i)_{jk}\,\omega_k$$

for $i, j = 1, \ldots, n$, and define the matrix T by

$$T_{jk} \;=\; \mathrm{tr}(\omega_j\omega_k) \;=\; \mathrm{tr}(W_jW_k).$$

Then, for $\alpha = x_1\omega_1 + \cdots + x_n\omega_n \in \mathcal{A}$, we have

$$\alpha \in \mathcal{T}_p \iff \sum T_{jk}x_k \equiv 0 \pmod{p} \text{ for } j = 1, \ldots, n.$$

Solving this system of congruences gives $\mathcal{T}_p$.

Proposition. *If $p > n$ then $\mathcal{R}_p = \mathcal{T}_p$.*

Proof. It is clear that $\mathcal{R}_p \subseteq \mathcal{T}_p$. Assume $p > n$ and take $\alpha \in \mathcal{T}_p$.

Let μ_α denote the minimal polynomial of α over $\mathbb{Q}$. Since

$$\mathrm{tr}(\alpha^k) \equiv 0 \pmod{p}$$

for all $k > 0$, it is a consequence of Newton's relations that

$$\mu_\alpha(x) \equiv x^m \pmod{p},$$

and therefore $\alpha \in \mathcal{R}_p$. □

Computing $[\mathcal{R}_p/\mathcal{R}_p]$.

Let the matrices $W_1, \ldots, W_n$ be defined as above. Take

$$\gamma \;=\; y_1\omega_1 + \cdots + y_n\omega_n \in \mathbb{Q}\mathcal{A} = \mathcal{K}$$

and set

$$C_\gamma \;=\; y_1W_1 + \cdots + y_nW_n.$$

The matrix C_γ expresses a $\mathbb{Z}$-basis for $\gamma\mathcal{A}$ in terms of $\omega_1, \ldots, \omega_n$.

If the matrix J expresses a $\mathbb{Z}$-basis for $\mathcal{R}_p$ in terms of $\omega_1, \ldots, \omega_n$ then $JC_\gamma J^{-1}$ gives a $\mathbb{Z}$-basis for $\gamma\mathcal{R}_p$ in terms of the basis for $\mathcal{R}_p$ expressed by J, and therefore

$$\gamma\mathcal{R}_p \subseteq \mathcal{R}_p \iff JC_\gamma J^{-1} \in \mathbb{Z}^{n\times n} \iff \sum y_i\,(JW_iJ^{-1}) \in \mathbb{Z}^{n\times n}.$$

Solving this set of n^2 relations for the unknowns $y_1, \ldots, y_n$ gives $[\mathcal{R}_p/\mathcal{R}_p]$.