1. Integral Bases

The arithmetic in global fields bases essentially on the notion of integral elements. This concept is a generalization of the rational integers $\mathbb{Z}$. Those can be viewed as the intersection of all valuation rings of $\mathbb{Q}$. For global function fields this must be replaced adequately since the intersection of all valuation rings is the field of constants, its quotient field is not the function field itself.

Definition 1.1. *We define as base ring R_0 either the rational integers (number field case) or the polynomial ring $\mathbb{F}_q[t]$ (function field case) and let F_0 be its field of quotients. For a finite extension E of F_0 we define $o_E := Cl(R_0, E)$ (***integral closure of** R_0 **in** E*) as the intersection of all valuation rings of E containing R_0.*

We remark that this definition can also be used for function fields over fields of characteristic zero. Our definition has the advantage that the integers of global fields automatically form a ring which satisfies $Cl(Cl(R_0, E), E) = Cl(R_0, E)$. Moreover, we have the following properties:

(i) R_0 coincides with its integral closure in its quotient field $F_0 = \mathcal{Q}(R_0)$. One says that R_0 is **integrally closed**. From the preceding remark we conclude that the integral closure of a ring in a field is integrally closed.

(ii) $Cl(R_1, E) \subseteq Cl(R_2, E)$ for $R_1 \subseteq R_2 \subseteq E$.

Definition 1.2. *An element x is said to be* **integral** *over R_0 if it is a zero of a monic polynomial $f(t) \in R_0[t]$ of positive degree.*

Lemma 1.3. *Let R be a valuation ring with quotient field F. Then R is integrally closed.*

Proof Let us assume that the element $0 \neq x$ of F is integral over R. Then it satisfies an equation

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} \;=\; 0 \;\; (a_i \in R) \;\; . \qquad (1)$$

If x is not contained in R we have $\varphi(x) > 1$ for the valuation φ belonging to R. But this implies $\varphi(a_i x^{n-i}) \leq \varphi(x)^{n-i} < \varphi(x)^n$ for $1 \leq i \leq n$ with the consequence

$$\varphi\left(\sum_{i=1}^{n} a_i x^{n-i}\right) < \varphi(x)^n$$

contradicting (1).

□

Lemma 1.4. *The integral elements x of a finite extension E of F_0 are exactly the elements of $Cl(R_0, E)$.*

Proof.
(i) We assume that

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} \;=\; 0 \;\; (a_i \in R_0\,,\; 1 \le i \le n) \tag{2}$$

for some natural number n. For any non-archimedian valuation v of E containing R_0 in its valuation ring we have $v(a_i) \le 1$. Hence, as a consequence of the strong triangular inequality, $v(x)$ also belongs to that valuation ring. This proves $x \in Cl(R_0, E)$.
(ii) We let $x \in Cl(R_0, E)$ and assume that there is no equation

$$1 \;=\; \sum_{i=1}^{n} a_i x^{-i} \;\; (n \in \mathbb{Z}^{>0},\; a_i \in R_0,\; 1 \le i \le n,\; a_n \ne 0) \;\; .$$

(This implies $x \ne 0$, but 0 is obviously integral over any ring. If x satisfies an equation of that type we can multiply it with x^n and obtain an equation which shows that x is integral over R_0.) The non existence of such an equation shows that $\sum_{i=1}^{\infty} R_0 x^{-i}$ is a proper ideal of the unital ring $R_0[x^{-1}]$. It is therefore contained in a maximal ideal $\mathfrak{m}$ of that ring. According to the Lemma of Chevalley there exists a valuation w of E with valuation ring R_w containing R_0 and valuation ideal containing $\mathfrak{m}$. This implies $w(x) > 1$, a contradiction to our assumption $x \in Cl(R_0, E)$.
□

The following criterion is useful for testing elements whether they are integral.

Lemma 1.5. *(***Kronecker's Criterion***)* *An element x is integral over R_0 if and only if there exist finitely many non-zero elements $\omega_1, ..., \omega_n$ satisfying $x(\omega_1, ..., \omega_n) = (\omega_1, ..., \omega_n)M$ with a matrix $M \in R_0^{n\times n}$.*

Proof. Clearly, we can assume that x is non-zero. If x is known to be a zero of a monic n-th degree polynomial $f(t) \in R_0[t]$ the powers x^m for $m \ge n$ can be expressed as linear combinations of $1, x, ..., x^{n-1}$ with coefficients in R_0. Hence, the elements $\omega_i = x^{i-1}$ $(1 \le i \le n)$ satisfy Kronecker's Criterion. On the other hand, if that criterion is satisfied the corresponding linear system of equations can be interpreted as an eigenvalue equation for x. Therefore x is a zero of the characteristic polynomial $\det(tI_n - M) \in R_0[t]$.
□

With Kronecker's Criterion it is easy to show that the sum and the product of two integral elements is integral again. Also, if x is a zero of a non-constant monic polynomial whose coefficients are integral then x is integral itself. We leave both tasks as an exercise for the reader.

We note that the algebraic elements over F_0 which are R_0-integral form a subring $\bar{R}_0$ of the algebraic closure $\bar{F}_0$.

For computations with the algebraic integers of a finite extension E of F_0 it is important that the ring $Cl(R_0, E)$ is a free R_0-module. Hence, fixing a basis, its elements can be represented as vectors of R_0^n for $n = [E : F_0]$. This is true since R_0 is a principal ideal ring. If the base ring does not have this property (for example, if we consider relative extensions) such a basis - usually called **integral basis** - need not exist. A unital subring S of E which is a free R_0-module of rank n is said to be an **R_0-order**.

For the following we must stipulate that E is separably generated over F_0. In the number field case this is guaranteed, of course. For function fields in non-zero characteristic this assumption is non-trivial.

Lemma 1.6. *Let K be a field of characteristic p with $K^p = K$. Let F be a finite extension of the function field $K(t)$ and η a K-transcendental element of F. Then F is separable over $K(\eta)$ if and only if η is not in F^p.*

Proof. If η belongs to F^p there exists an element ξ in F with $\eta = \xi^p$. Its minimal polynomial over $K(\eta)$ is therefore $m_{\xi/K(\eta)}(t) = t^p - \eta$ and ξ is inseparable over $K(\eta)$.
On the other hand, if F is inseparable over $K(\eta)$ then we have $K(\eta) \subseteq F_{sep} \subset F$ and F has degree $q := p^m$ over F_{sep}. The minimal polynomial of an element α of F over F_{sep} is of the form

$$m_{\alpha/F_{sep}}(t) \; = \; t^{p^l} - a \;\; (a \in F_{sep}, \; 0 \leq l \leq m)$$

from which we conclude that F^q is contained in F_{sep}. We will show that both fields actually coincide which finishes the proof.
We first show that

$$[F^q : K(\eta)^q] = [F : K(\eta)] \; . \qquad (3)$$

Let us assume that F is of degree r over $K(\eta)$. Then we have $F = K(\eta)\omega_1 + ... + K(\eta)\omega_r$ for suitable elements $\omega_1, ..., \omega_r$ of F. This yields

$F^q = K(\eta)^q\omega_1^q + ... + K(\eta)^q\omega_r^q$, hence $[F^q : K(\eta)^q] \leq r$. The equations

$$\begin{aligned} 0 &= \sum_{i=1}^{r} \lambda_i^q \omega_i^q \\ &= \left(\sum_{i=1}^{r} \lambda_i \omega_i \right)^q \end{aligned}$$

with coefficients $\lambda_i \in K(\eta)$ show that the ω_i^q are also $K(\eta)^q$-linearly independent.
From our premises we know that $K^q = K$ and obtain $K(\eta)^q = K(\eta_0)$ for $\eta_0 := \eta^q$. The polynomial $t^q - \eta_0$ is irreducible in $K(\eta_0)[t]$ implying $[K(\eta) : K(\eta_0)] = q$. From

$$[F : F^q][F^q : K(\eta)^q] = [F : K(\eta)^q] = [F : K(\eta)][K(\eta) : K(\eta)^q]$$

and (3) we finally get

$$[F : F^q] \;=\; q \;\;.$$

□

Corollary 1.7. *Any finite extension of F_0 can be separately generated.*

From now on we therefore assume that E is a separable extension of degree n of F_0. Then we have $E = F_0(\alpha)$ with an element α whose minimal polynomial $m_{\alpha/F_0}(x) \in F_0[x]$ is of degree n. Clearing denominators we obtain $am_{\alpha/F_0}(x) \in R_0[x]$ for a suitable element $a \in R_0$. Multiplication by a^{n-1} and replacement of x by ax yields a monic irreducible polynomial for $a\alpha$ which again generates E over F_0 and is integral over R_0. Hence, without loss of generality we can assume that a generating element of E over F_0 is integral over R_0.

Clearly, the ring $S := R_0[\alpha]$ is a subring of E consisting of R_0-integral elements. It is therefore contained in the maximal order $o_E := Cl(R_0, E)$. S is also an R_0-order. We want to show that the same holds for o_E. We note that the **trace bilinar form**

$$\mathrm{Tr} \;:\; E \times E \;:\; (x, y) \mapsto \mathrm{Tr}(xy)$$

is non degenerate. Namely, we have $x = \sum_{i=1}^{n} \xi_i \alpha^{i-1}$, $y = \sum_{j=1}^{n} \eta_j \alpha^{j-1}$ and therefore $\mathrm{Tr}(xy) = (\xi_1, ..., \xi_n)A(\eta_1, ...\eta_n)^{tr}$ for the matrix A with entries $a_{ij} = \mathrm{Tr}(\alpha^{i+j-1})$. The determinant of A is easily seen to be of Vandermonde's type. It is non zero since the minimal polynomial of α does not have multiple roots.

We define the dual R_0-module for any R_0-module S via

$$S^\star := \{y \in E \mid \mathrm{Tr}(xy) \in R_0 \; \forall x \in S\} \;\;.$$

For any R_0-basis $\tau_1, ..., \tau_n$ of S there exists the dual basis $\tau_1^\star, ..., \tau_n^\star$ defined by the linear system of equations $\mathrm{Tr}(\tau_i \tau_j^\star) = \delta_{ij}$ $(1 \le i, j \le n)$. An easy computation shows that the transformation matrix from the $\tau_i^\star$ to the τ_i has determinant $\det(A)$. Because of $Cl(R_0, E) \subseteq S^\star$ we obtain that $Cl(R_0, E)$ is indeed an R_0-order and that determinant gives further information about the maximal order. We note that the square of the determinant of a transformation matrix from a basis of $CL(R_0, E)$ to a basis of $R_0[\alpha]$ divides $\det(A)$. That determinant is also called **discriminant** of the equation order $R_0[\alpha]$. Similarly, the **discriminant** of an R_0-order S with basis $\tau_1, ..., \tau_n$ is defined as the determinant of the matrix with entries $Tr(\tau_i \tau_j)$ $(1 \le i, j \le n)$.

Since R_0 is a unique factorisation domain (even a Eucliden ring) the discriminants $d(S)$ of S and d_E of o_E have unique factorisations up to units and the index $(o_F : S)$ is necessarily a product of primes of R_0 whose squares divide $d(S) = d(m_\alpha)$.

We therefore let $\mathcal{S} = \{\pi_1, ..., \pi_s\}$ denote the set of primes π of R_0 for which π^2 divides $d(S)$. For each prime π_j we calculate the so-called **π_j-maximal overorder** S_j of S characterized by the properties $\pi_j \not| (o_F : S_j)$ and $(S_j : S)$ is a power of π_j. Merging the π_j-maximal overorders S_j for $j = 1, ..., s$ finally yields o_F.

We still need to develop methods for determining π-maximal overorders Λ_π of a given order Λ, usually the equation order with which we start. For this we recall a few important results about unital commutative rings R. The set $\mathcal{N}$ consisting of all nilpotent elements of R is called the **nilradical** of R. It is easy to see that $\mathcal{N}$ is an ideal and that the nilradical of $R/\mathcal{N}$ is zero. We claim that $\mathcal{N}$ is the intersection of all prime ideals of R. Indeed, for $x \in \mathcal{N}$ a suitable power, say x^k, vanishes. Hence, x belongs to every prime ideal of R. The other direction is more complicated. We assume that there exists an element x which is contained in every prime ideal of R but which is not nilpotent. The set $\mathcal{M}$ of all ideals $\mathfrak{a}$ of R subject to $x^n \notin \mathfrak{a}$ $\forall n \in \mathbb{N}$ is not empty since it contains the zero ideal. According to Zorn's lemma $\mathcal{M}$ contains a maximal element, say $\mathfrak{p}$. Obviously, $\mathfrak{p}$ does not contain x. For all $u, v \in R \setminus \mathfrak{p}$ we have $\mathfrak{p} \subset \mathfrak{p} + Ru$, $\mathfrak{p} + Rv$, hence there exist powers $x^k \in \mathfrak{p} + Ru$, $x^l \in \mathfrak{p} + Rv$. This yields $x^{k+l} \in \mathfrak{p} + Ruv$ and consequently $uv \notin \mathfrak{p}$, i.e. $\mathfrak{p}$ is a prime ideal not containing x. This contradicts our assumption.

The intersection of all maximal ideals of R is called the **Jacobson radical** J_R of R. We claim that an element $x \in R$ belongs to J_R precisely, if $1 - xy$ is a unit of R for all $y \in R$. If $1 - xy$ is not a unit, it belongs to a suitable maximal ideal, say $\mathfrak{m}$. For $x \in J_R \subseteq \mathfrak{m}$ we obtain

$xy \in \mathfrak{m}$ and therefore $1 \in \mathfrak{m}$, a contradiction. If x is not contained in some maximal ideal $\mathfrak{m}$ we have $\mathfrak{m} + Rx = R$, hence $m + yx = 1$ for appropriate elements $m \in \mathfrak{m}$, $y \in R$. But then the element $1 - yx = m$ belongs to $\mathfrak{m}$ and cannot be a unit.

Lemma 1.8. *(***Nakayama***) Let M be a finitely generated unitary R-module and $\mathfrak{a}$ an ideal of R which is contained in the Jacobson radical of R and satisfies $\mathfrak{a}M = M$. Then the module M is trivial.*

Proof. We assume that M is non-zero and that $u_1, ..., u_n$ is a minimal number of generators for M. Because of $u_n \in M = \mathfrak{a}M$ there exist elements $a_1, ..., a_n \in \mathfrak{a}$ with $u_n = a_1u_1 + ... + a_nu_n$. Since $\mathfrak{a}$ is contained in the Jacobson radical of R the element $1 - a_n$ is a unit of R and we obtain

$$u_n = a_1(1 - a_n)^{-1}u_1 + ... + a_{n-1}(1 - a_n)^{-1}u_{n-1}$$

contrary to our assumption.
□

Lemma 1.9. *Let R be an entire noetherian local ring and $\mathfrak{a}$ a proper ideal of R. Then we have $\mathfrak{a}^{n+1} \subset \mathfrak{a}^n$ for all natural numbers n.*

Proof. Let $\mathfrak{m}$ denote the maximal ideal of R. Clearly, $\mathfrak{a}$ is contained in $\mathfrak{m} = J_R$. If we had $\mathfrak{a}\mathfrak{a}^n = \mathfrak{a}^n$ we would obtain $\mathfrak{a}^n = 0$ by Nakayama's lemma. But $\mathfrak{a}$ contains non-zero elements, and so does $\mathfrak{a}^n$ since R is entire.
□

Lemma 1.10. *Let R be an entire noetherian ring and $\mathfrak{a}$ a proper ideal of R. Then we have $\mathfrak{a}^{n+1} \subset \mathfrak{a}^n$ for all natural numbers n.*

Proof. We apply localisation! Let $\mathfrak{a}$ be contained in the maximal ideal $\mathfrak{p}$ of R. If we had $\mathfrak{a}\mathfrak{a}^n = \mathfrak{a}^n$ the same would hold for the ideal $\tilde{\mathfrak{a}} = \frac{\mathfrak{a}}{R \backslash \mathfrak{p}}$. One easily sees that $\widetilde{\mathfrak{a}^{n+1}} = \tilde{\mathfrak{a}}\widetilde{\mathfrak{a}^n}$ and the proof is finished by an application of the preceding lemma.
□

Definition 1.11. *Let Λ be a commutative unital ring and $\mathfrak{a}$ be an ideal of Λ. We define the* **$\mathfrak{a}$-radical** *of Λ as the set $J_\mathfrak{a}$ of all elements x of Λ for which a suitable power x^k belongs to $\mathfrak{a}$.*

We note that the elements of $J_\mathfrak{a}$ are exactly the representatives of the nilpotent residue classes in $\Lambda/\mathfrak{a}$. Hence, $J_\mathfrak{a}$ is the intersection of all prime ideals of Λ containing $\mathfrak{a}$.

Definition 1.12. *Let Λ be an order of our global field F and $\mathfrak{a}$ a non-zero ideal of Λ. We define the* **ring of multipliers** *of $\mathfrak{a}$ as $[\mathfrak{a}/\mathfrak{a}] := \{x \in F \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$.*

It is immediate that $[\mathfrak{a}/\mathfrak{a}]$ is a ring containing Λ. Since the ideal $\mathfrak{a}$ has an R_0-basis the Kronecker criterion tells us that any multiplier of $\mathfrak{a}$ is an algebraic integer of F. Hence, the ring of multipliers is itself an order of F lying between Λ and o_F. We apply these concepts in the following situation.

The ideal $\mathfrak{a}$ is chosen as $\pi\Lambda$. The corresponding radical $J_{\pi\Lambda}$ certainly contains $\pi\Lambda$ and the latter is of index π^n in Λ. We want to prove that

$$J_{\pi\Lambda} = \{x \in \Lambda \mid x^n \in \pi\Lambda\} \quad . \tag{4}$$

The successive powers of $J_{\pi\Lambda}$ form a strongly decreasing chain of ideals. Since there is a positive integer, say m, such that the m-th power of each R_0-basis element of $J_{\pi\Lambda}$ is in $\pi\Lambda$ the nm-th power $J_{\pi\Lambda}^{mn}$ is contained in $\pi\Lambda$. This and the usual index estimates yield (4).

The following important lemma is due to Zassenhaus.

Lemma 1.13. *Let Λ be an order of F and π be a prime of R_0. Then $[J_{\pi\Lambda}/J_{\pi\Lambda}]$ is an overorder of Λ. The index $([J_{\pi\Lambda}/J_{\pi\Lambda}] : \Lambda)$ is a power of π. Especially, Λ is π-maximal precisely if it coincides with $[J_{\pi\Lambda}/J_{\pi\Lambda}]$.*

Proof. Any $x \in [J_{\pi\Lambda}/J_{\pi\Lambda}]$ satisfies $xJ_{\pi\Lambda} \subseteq J_{\pi\Lambda}$. For $\pi \in J_{\pi\Lambda}$ we obtain $x\pi \in J_{\pi\Lambda} \subseteq \Lambda$, hence $x \in \pi^{-1}\Lambda$. Therefore we have $\pi^{-1}\Lambda \supseteq [J_{\pi\Lambda}/J_{\pi\Lambda}] \supseteq \Lambda$ from which the first part of the lemma follows.

Concerning the π-maximality of Λ we assume that Λ is a proper subset of the π-maximal overorder Λ_π and need to show $\Lambda \subset [J_{\pi\Lambda}/J_{\pi\Lambda}]$.

Let κ be the smallest exponent with $\pi^\kappa\Lambda_\pi \subseteq J_{\pi\Lambda}$. Since sufficiently large powers of $J_{\pi\Lambda}$ are contained in $\pi\Lambda$ there is a smallest natural number, say μ, with $J_{\pi\Lambda}^{\mu}\Lambda_\pi \subseteq J_{\pi\Lambda}$. In case $\mu = 1$ we obtain $\Lambda_\pi \subseteq [J_{\pi\Lambda}/J_{\pi\Lambda}]$, hence equality holds, and we indeed have $\Lambda \subset [J_{\pi\Lambda}/J_{\pi\Lambda}]$. In case $\mu > 1$ we have $J_{\pi\Lambda}^{\mu-1}\Lambda_\pi \not\subseteq J_{\pi\Lambda}$. We choose $x \in J_{\pi\Lambda}^{\mu-1}\Lambda_\pi \setminus J_{\pi\Lambda}$. Clearly, x belongs to $[J_{\pi\Lambda}/J_{\pi\Lambda}]$. Since x^2 is in $J_{\pi\Lambda}$ a suitable power of x is in $\pi\Lambda$. In case of $x \in \Lambda$ we had $x \in J_{\pi\Lambda}$, a contradiction to the choice of x.

□

The lemma also provides an algorithm for actually calculating Λ_π. We just need to solve two tasks:

(1) compute the π-radical of an order,
(2) compute the ring of multipliers of that π-radical.

After each step we have either increased the order or we know that the considered order is already π-maximal.

There are two solutions for the first task depending on whether the characteristic of $\Lambda/\pi\Lambda$ is larger than n. For a smaller characteristic we use linear algebra to determine a basis of the kernel of the homomorphism

$$\varphi : \Lambda/\pi\Lambda \to \Lambda/\pi\Lambda : x \mapsto x^{p^\kappa} \tag{5}$$

where the exponent κ is chosen subject to $p^{\kappa-1} < n \le p^\kappa$.

Example The polynomial $f(t) = t^3 + 17t^2 - 2t + 9 \in \mathbb{Z}[t]$ is irreducible with discriminant $d(f) = -3^2 5^3 163$. We start with the equation order $\Lambda = \mathbb{Z}[\rho]$ for a zero $\rho \in \mathbb{C}$. For the computation of the corresponding maximal order we need to determine the p-maximal overorders Λ_p for $p = 3$ and $p = 5$.
All elements of $F = \mathbb{Q}(\rho)$ are presented in the form $\xi = x_1 + x_2\rho + x_3\rho^2$ with a vector of coefficients $\mathbf{x} = (x_1, x_2, x_3)^{tr} \in \mathbb{Q}^3$. Because of 3 not being larger than the degree of the extension $F/\mathbb{Q}$ we determine the 3-radical $J_{3\Lambda}$ of Λ via the kernel of φ in (5). We note that we can choose $\kappa = 1$ in this case. Upon reducing the coefficients modulo 3 the images of the basis elements $1, \rho, \rho^2$ become

$$1,\ \rho^3 = \rho^2 - \rho,\ \rho^6 = -\rho^2 + \rho\ .$$

Hence, that kernel is of dimension one with generating element $\rho^2 + \rho$. Computing the Hermite normal form of the 3×4 matrix whose columns are the vectors of coefficients of that element and of the generators for 3Λ we obtain the basis

$$\alpha_1 = 3,\ \alpha_2 = 3\rho,\ \alpha_3 = \rho^2 + \rho$$

for $J_{3\Lambda}$. Next we compute the ring of multipliers $T := [J_{3\Lambda}/J_{3\Lambda}]$. $\xi = x_1 + x_2\rho + x_3\rho^2$ belongs to T if and only if the elements $\xi\alpha_i$ are in $J_{3\Lambda}$ for $i = 1, 2, 3$. We therefore compute matrices $M_{\alpha_i} \in \mathbb{Z}^{3\times 3}$ such that

$$\alpha_i(1, \rho, \rho^2) \ = \ (\alpha_1, \alpha_2, \alpha_3) M_{\alpha_i}$$

and obtain

$$M_{\alpha_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 3 \end{pmatrix},\ M_{\alpha_2} = \begin{pmatrix} 0 & 0 & -9 \\ 1 & -1 & 19 \\ 0 & 3 & -51 \end{pmatrix},\ M_{\alpha_3} = \begin{pmatrix} 0 & -3 & 48 \\ 0 & 6 & -105 \\ 1 & -16 & 274 \end{pmatrix}.$$

Then we apply row reduction to the rows of all 3 matrices. Because of $T \subseteq \frac{1}{3}\Lambda$ we can add the rows $(3\ 0\ 0)$, $(0\ 3\ 0)$, $(0\ 0\ 3)$ so that the reduction is carried out essentially in $\mathbb{Z}/3\mathbb{Z}$ which keeps the intermediate entries small. The remaining non–zero rows become

$$(1\ 0\ 0)\ ,\ (0\ 1\ -1)\ ,\ (0\ 0\ 3)\ .$$

Obviously, a basis for the solution space

$$\{\mathbf{x} \mid (1, \rho, \rho^2)\mathbf{x} \in T\}$$

is

$$\mathbf{x}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ \mathbf{x}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{x}_3 = \begin{pmatrix} 0 \\ 1/3 \\ 1/3 \end{pmatrix} .$$

The result is the 3–maximal overorder of Λ:

$$\Lambda_3 = [J_{3\Lambda}/J_{3\Lambda}] = \mathbb{Z} + \mathbb{Z}\rho + \mathbb{Z}\frac{\rho^2+\rho}{3} .$$

We generalize these ideas and describe a method for computing the ring of multipliers

$$[\mathfrak{a}/\mathfrak{b}] = \{\xi \in \mathcal{Q}(R) \mid \xi\mathfrak{b} \subseteq \mathfrak{a}\}$$

for two ideals $\mathfrak{a} = R_0\alpha_1 + \ldots + R_0\alpha_n$ and $\mathfrak{b} = R_0\beta_1 + \ldots + R_0\beta_n$ of an order $R = R_0\gamma_1 + \ldots + R_0\gamma_n$. We assume that we know the corresponding transformation matrices $T_{\gamma,\alpha}$ and $T_{\gamma,\beta}$ satisfying

$$\begin{array}{l} (\alpha_1, \ldots, \alpha_n) = (\gamma_1, \ldots, \gamma_n)T_{\gamma,\alpha} \\ (\beta_1, \ldots, \beta_n) = (\gamma_1, \ldots, \gamma_n)T_{\gamma,\beta} \end{array}$$

and that both matrices are upper triangular matrices, more precisely, that they are in column reduced Hermite normal form.

We represent $\xi \in [\mathfrak{a}/\mathfrak{b}]$ in the form $\xi = \sum_{i=1}^{n} x_i\gamma_i$ with coefficients $x_i \in F_0$. Then the following criterion is immediate:

$$\xi\mathfrak{b} \subseteq \mathfrak{a} \Leftrightarrow \xi\beta_i \in \mathfrak{a} \quad (1 \le i \le n). \tag{6}$$

We write

$$\begin{aligned} \beta_i\xi &= \beta_i(\gamma_1, \ldots, \gamma_n)\mathbf{x} \\ &= (\gamma_1, \ldots, \gamma_n)\tilde{M}_i\mathbf{x} \quad \text{with} \quad \tilde{M}_i \in F_0^{n\times n} \\ &= (\alpha_1, \ldots, \alpha_n)T_{\gamma,\alpha}^{-1}\tilde{M}_i\mathbf{x} \ . \end{aligned}$$

We put $M_i = T_{\gamma,\alpha}^{-1}\tilde{M}_i$ and note that $\det(M_i) \neq 0$. The condition (6) now becomes

$$M_i\mathbf{x} \in R_0^{n\times 1} \quad (1 \le i \le n) , \tag{7}$$

or

$$\Gamma\mathbf{x} \in R_0^{n^2\times 1} \tag{8}$$

with

$$\Gamma = \begin{pmatrix} M_1 \\ \vdots \\ M_n \end{pmatrix} . \tag{9}$$

Let b_0 be the least common multiple of the denominators of the entries of Γ. Then

$$b_0\Gamma \in R_0^{n^2 x\, n}$$

and equation (8) becomes

$$b_0\Gamma\mathbf{x} \in b_0 R_0^{n^2\times 1} \quad .$$

Then we compute the (row reduced) Hermite normal form of $b_0\Gamma$. In order to avoid the usual growth of intermediate entries we observe the following.

We let $b \in \mathfrak{b} \cap R_0$. An element $\xi \in [\mathfrak{a}/\mathfrak{b}]$ clearly maps b into $\mathfrak{a} \subseteq R$. We therefore know that $\xi \in \frac{1}{b}R$ or $b\xi \in R$. Hence, we extend the matrix Γ by adding n additional rows representing bI_n, I_n the $n \times n$ unit matrix. In the subsequent Hermite normal form computation of an $(n^2+n)\times n$ matrix all entries stay bounded by the size of b, respectively $b_0 b$.

We denote the matrix consisting of the first n rows of the Hermite normal form of $b_0\Gamma$ by M. Again, M is a regular upper triangular matrix. Then $\mathbf{x} \in R_0^{n\times 1}$ satisfies $M_i\mathbf{x} \in R_0^{n\times 1} \quad (1 \le i \le n)$ if and only if $M\mathbf{x} \in b_0 R_0^{n\times 1}$. The vector $\mathbf{x}$ is therefore of the form

$$\mathbf{x} = b_0 M^{-1}\mathbf{y} \text{ with } \mathbf{y} \in R_0^{n\times 1} \quad .$$

It is therefore an R_0-linear combination of the columns of the matrix $b_0 M^{-1}$. Hence, the elements $\eta_1, \dots, \eta_n$ satisfying

$$(\eta_1, \dots, \eta_n) = (\gamma_1, \dots, \gamma_n)\ b_0 M^{-1} \tag{10}$$

form an R_0-basis of $[\mathfrak{a}/\mathfrak{b}]$.

For $p > n$ there is a more efficient way of computing the p–radical of an order Λ.

Proposition 1.14. *Let Λ be an order of E. Let π be a prime of R_0 and $p = \pi$ (number field case) or let p denote the characteristic of F_0 (function field case). For $p > n = [E : F_0]$ we have $J_{\pi\Lambda} = \{x \in \Lambda \mid \mathrm{Tr}(xy) \in \pi R_0\ \forall y \in \Lambda\}$.*

Proof. We recall that $J_{\pi\Lambda}$ is the intersection of all prime ideals of Λ containing π, say $\mathfrak{p}_1, ..., \mathfrak{p}_s$. (We note that there can exist only finitely many such ideals since the corresponding residue class ring is finite and therefore admits only finitely many prime ideals.) Let Γ be the Galois closure of E and choose automorphisms $\sigma_1, ..., \sigma_n$ of Γ such that $\sigma_i\mid_E \quad (1 \le i \le n)$ are the pairwise different embeddings of E into Γ. For any $y \in E$ we have $\mathrm{Tr}(y) = \sum_{i=1}^{n} \sigma_i(y)$. For $y \in \Lambda$ and $x \in J_{\pi\Lambda}$ we get $xy \in J_{\pi\Lambda} = \prod_{j=1}^{s} \mathfrak{p}_j$. Let $\mathfrak{P}_1, ..., \mathfrak{P}_u$ be all prime ideals of $Cl(\Lambda, \Gamma)$ containing π. Each of those contains exactly one of the prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_s$. Ordering them adequately, we get

$$\pi \in \mathfrak{p}_i \subseteq \mathfrak{P}_{i_j}$$

with

$$\mathfrak{p}_i \subseteq \bigcap_{j=1}^{m_i} \mathfrak{P}_{i_j}$$

and

$$\{\mathfrak{P}_{i_j} \mid 1 \leq i_j \leq m_i,\ 1 \leq i \leq s\} \ = \ \{\mathfrak{P}_1, ..., \mathfrak{P}_u\} \ .$$

Hence, xy is contained in the product $\Pi := \prod_{j=1}^{u} \mathfrak{P}_j$, too. Since the automorphisms σ_i permute the set $\{\mathfrak{P}_1, ..., \mathfrak{P}_u\}$ every conjugate $\sigma_i(xy)$ is contained in Π as well. Therefore we obtain $\mathrm{Tr}(xy) \in \Pi \cap R_0 \ = \ \pi R_0$.

On the other hand, every element z of $\{x \in \Lambda \mid \mathrm{Tr}(xy) \in \pi R_0 \ \forall y \in \Lambda\}$ satisfies $\mathrm{Tr}(z^j) \in \pi R_0$ for all $j \in \mathbb{N}$. Then Newton's relations between the traces $S_i := \mathrm{Tr}(z^i)$ and the coefficients $(-1)^i \sigma_i$ of the powers t^{n-i} of the characteristic polynomial of z:

$$\sum_{i=0}^{k-1} (-1)^i \sigma_i S_{k-i} \ + \ (-1)^k k \sigma_k \ = \ 0 \ \ (\sigma_0 := 1\,,\ 0 \leq k \leq n)$$

and

$$\sum_{i=0}^{n} (-1)^i \sigma_i S_{k-i} \ = \ 0 \ \ (\sigma_0 := 1\,,\ n \leq k)$$

tell us that the coefficients of the characteristic polynomial of z are in πR_0, too. (Here we need our assumption $p > n$.) This has the consequence $z^n \in \pi\Lambda$, hence $z \in J_{\pi\Lambda}$.

□

Example We continue the example from above, this time computing the 5–radical of $\Lambda = \mathbb{Z}[\rho]$. Since the trace is $\mathbb{Q}$–linear we need to determine all $x = x_1 + x_2\rho + x_3\rho^2 \in \Lambda$ satisfying $\mathrm{Tr}(x\rho^j) \in 5\mathbb{Z}$ $(j = 0, 1, 2)$. For this we compute the values

$$\mathrm{Tr}(1) \ = \ 3 \ , \qquad (11)$$

$$\mathrm{Tr}(\rho) \ = \ -17 \ , \qquad (12)$$

$$\mathrm{Tr}(\rho^2) \ = \ 293 \ , \qquad (13)$$

$$\mathrm{Tr}(\rho^3) \ = \ -5042 \ , \qquad (14)$$

$$\mathrm{Tr}(\rho^4) \ = \ 86453 \ . \qquad (15)$$

Again we remark that we only need these values modulo 5. The condition $\mathrm{Tr}(x\rho^j) \in 5\mathbb{Z}$ $(j = 0, 1, 2)$ amounts to $3x_1 - 2x_2 + 3x_3 \equiv 0 \bmod 5$. Hence, the elements 5, $\rho - 1$, $\rho^2 - \rho$ form a $\mathbb{Z}$–basis of $J_{5\Lambda}$.

For the computation of the ring of multipliers of the π–radical there is still another method valid only for equation orders. In this case all elements can be presented via specializations $t \mapsto \rho$ of polynomials of $R_0[t]$. Since we frequently need to switch from polynomials in $R_0[t]$ to their images in $(R_0/\pi R_0)[t]$ and vice versa we stipulate that all occuring polynomials are in $R_0[t]$. The generating polynomial $f(t) \in R_0[t]$ is monic and separable. In $(R_0/\pi R_0)[t]$ it decomposes into a product of monic irreducible polynomials $p_i(t) \in R_0[t]$:

$$f(t) \;\equiv\; \prod_{i=1}^{s} p_i(t)^{e_i} \bmod \pi R_0[t] \;\; . \tag{16}$$

We note that the $p_i(t)$ remain irreducible modulo $\pi R_0[t]$. Since π^2 divides the discriminant of $f(t)$ at least one exponent e_i is bigger than one. For the following we do not even need the last factorisation. We only need the weaker one

$$f(t) \;\equiv\; \prod_{i=1}^{s} g_i(t)^{i} \bmod \pi R_0[t] \;\; , \tag{17}$$

with $g_i(t)$ being the product of all $p_j(t)$ for which e_j equals i. That last factorisation can be obtained just by calculations of the greatest common divisors of polynomials and their derivatives and quotients of polynomials modulo $\pi R_0[t]$ (so-called **divisor cascading** or **factor refinement**). We note that the polynomials $g_i(t)$ are pairwise coprime modulo $\pi R_0[t]$. We also put

$$g(t) \;:=\; q\prod_{i=1}^{s} g_i(t) \;\in R_0[t] \;\; . \tag{18}$$

Lemma 1.15. *(***Dedekind Test***) Let Λ be the equation order $R_0[\rho]$ for a zero ρ of $f(t)$. Then the π–radical of Λ is given by*

$$J_{\pi\Lambda} \;=\; \pi\,\Lambda \,+\, g(\rho)\,\Lambda \;\; . \tag{19}$$

Define the polynomial $h(t)$ by

$$h(t) \;:=\; \frac{1}{\pi}(f(t) - \prod_{i=1}^{n} g_i(t)^{i}) \in R_0[t] \;\; . \tag{20}$$

Then the equation order is π–maximal if and only if the greatest common divisor of the polynomials $h(t)$ and $g(t)/g_1(t)$ in $(R_0/\pi R_0)[t]$ is one.
The proof also yields an R_0–basis of the ring of multipliers $T := [J_{\pi\Lambda}/J_{\pi\Lambda}]$ of the π–radical $J_{\pi\Lambda}$ which is useful if T is strictly larger than Λ.

Proof Since $f(t)$ divides $g(t)^n$ modulo $\pi R_0[t]$ we have $g(t)^n = f(t)A(t)+\pi B(t)$ for appropriate polynomials $A(t), B(t) \in R_0[t]$. Hence, $g(\rho)^n$ is in $\pi\Lambda$ and therefore $g(\rho)$ in $J_{\pi\Lambda}$. Consequently, the right-hand side of (19) is contained in $J_{\pi\Lambda}$.

On the other hand, if γ is in $J_{\pi\Lambda}$ then it is nilpotent modulo $\pi\Lambda$. We let $A(t) \in R_0[t]$ of degree less than n such that $\gamma = A(\rho)$. By long division we get $A(t)^n = q(t)f(t) + r(t)$ with $\deg(r) < \deg(f)$ in $R_0[t]$. Because of $A(\rho)^n \equiv 0 \bmod \pi\Lambda$ the polynomial $r(t)$ must be in $\pi R_0[t]$ and therefore $f(t)$ divides $A(t)^n$ modulo $\pi R_0[t]$. But then also $g(t)$ divides $A(t)$ modulo $\pi R_0[t]$. Hence, we get $\gamma + \pi\Lambda = (g(\rho) + \pi\Lambda)(k(\rho) + \pi\Lambda)$ for a suitable $k(t) \in R_0[t]$ and γ is contained in the right-hand side of (19).

In the remainder of the proof all occuring polynomials $A_i(t)$ are in $R_0[t]$.

The structure of the π–radical immediately tells us that $x \in F$ belongs to the ring of multipliers $T := [J_{\pi\Lambda}/J_{\pi\Lambda}]$ if and only if $x\pi$ and $xg(\rho)$ both belong to $J_{\pi\Lambda}$. We know that $T \subseteq \frac{1}{\pi}\Lambda$. Any element x of $\frac{1}{\pi}\Lambda$ can be written as $x = A(\rho)/\pi$ with a polynomial $A(t) \in R_0[t]$ of degree less than n. We will show that such an element belongs to T if and only if it satisfies the two conditions

(1) The polynomial $g(t)$ divides $A(t)$ modulo $\pi R_0[t]$;
(2) the polynomial $H(t)K(t)$ divides $A(t)$ modulo $\pi R_0[t]$, where $H(t)$ and $K(t)$ are defined by $H(t) \equiv f(t)/g(t) \bmod \pi R_0[t]$ and $K(t) \equiv g(t)/\gcd(h(t), g(t)) \bmod \pi R_0[t]$.

The first condition is obviously tantamount to $x\pi \in J_{\pi\Lambda}$. The second is derived from $xg(\rho) \in J_{\pi\Lambda}$ in the following way. According to (19) we have $xg(\rho) \in J_{\pi\Lambda}$ if and only if there exist polynomials $A_2(t), A_3(t) \in R_0[t]$ satisfying $A(\rho)g(\rho) = \pi(\pi A_2(\rho) + g(\rho)A_3(\rho))$. Again this is tantamount to

$$A(t)G(t) = \pi^2 A_2(t) + \pi g(t)A_3(t) + f(t)A_4(t) \tag{21}$$

with a suitable polynomial $A_4(t) \in R_0[t]$. This yields

$$A(t) \equiv A_4(t)\frac{f(t)}{g(t)} \bmod \pi R_0[t] \quad ,$$

and we define $H(t) \in R_0[t]$ via

$$H(t) \equiv f(t)/g(t) \bmod \pi R_0[t] \quad . \tag{22}$$

Then we have $A(t) = A_4(t)H(t) + \pi A_5(t)$. Inserting this into (21) we get

$$(g(t)H(t) - f(t))A_4(t) \;=\; \pi^2 A_2(t) + \pi g(t)(A_3(t) - A_5(t))$$

and with the notation of the lemma $h(t)A_4(t) = \pi A_2(t) + g(t)A_6(t)$. Since $g(t)$ therefore divides $h(t)A_4(t)$ modulo $\pi R_0[t]$ the polynomial $K(t)$ satisfying

$$K(t) \equiv \frac{g(t)}{\gcd(h(t), g(t))} \bmod \pi R_0[t] \tag{23}$$

divides $A_4(t)$ modulo $\pi R_0[t]$. Hence, we obtain $A_4(t) = K(t)A_7(t) + \pi A_8(t)$ and from this also

$$A(t) \;=\; H(t)K(t)A_7(t) \;+\; \pi(H(t)A_8(t) + A_5(t)) \;\;.$$

We conclude that the least common multiple of $g(t)$ and $H(t)K(t)$ modulo $\pi R_0[t]$ divides $A(t)$ modulo $\pi R_0[t]$. The following equations are valid in $(R_0/\pi R_0)[t]$:

$$\begin{aligned}
\operatorname{lcm}(g, HK) &= K \operatorname{lcm}(\gcd(h, g), H) \;\text{ by (23)} \\
&= \frac{g}{\gcd(h, g)} \frac{\gcd(h, g)H}{\gcd(h, g, H)} \\
&= \frac{f}{\gcd(h, g, H)} \\
&=: U \;\;.
\end{aligned}$$

Again the polynomial $U(t)$ is assumed to be in $R_0[t]$. It divides $A(t)$ modulo $\pi R_0[t]$.

We conclude that T coincides with Λ precisely for $\gcd(h, G, H) \equiv 1 \bmod \pi R_0[t]$. With respect to the notation of the lemma we remark that the greatest common divisor of G and H in $(R_0/\pi R_0)[t]$ equals the polynomial $G_1(t) := \prod_{i=2}^{n} g_i(t)$ modulo $\pi R_0[t]$. If the greatest common divisor of h and G_1 modulo $\pi R_0[t]$ is of degree $m \geq 1$, however, an R_0–basis of T is given by

$$1, \rho, ..., \rho^{n-m-1}, \frac{1}{\pi}U(\rho), \rho\frac{1}{\pi}U(\rho), ..., \rho^{m-1}\frac{1}{\pi}U(\rho) \;\;.$$

For $m \geq 1$ the index of Λ in T is therefore π^m.

□

Example We continue our example for $p = 5$. The polynomial $f(t) = t^3 + 17t^2 - 2t + 9$ splits modulo 5 into

$$f(t) \;\equiv\; (t-1)^3 \bmod 5\mathbb{Z}[t] \;\;.$$

We note that in the notation of 17 we have $g_1(t) = g_2(t) = 1$, $g_3(t) = (t-1) = G(t)$. In Dedekind's Lemma the polynomial $h(t)$ becomes $h(t) = ((t-1)^3 - f(t))/5 = -(4t^2 - t + 2)$. We easily see that $h(t) \equiv (t-1)(t+2) \bmod 5\mathbb{Z}[t]$. The greatest common divisor modulo $5\mathbb{Z}[t]$ of

$h(t)$ and $g_2(t)g_3(t)$ becomes $t-1$, the equation order is clearly not 5–maximal. We compute $U(t)=(t-1)^2$, $m=1$ and obtain the following $\mathbb{Z}$–basis of the ring of multipliers T:

$$1,\ \rho,\ (\rho^2-2\rho+1)/5 \ \ .$$

Once we have calculated the π-maximal overorders S_π for each prime element $\pi \in \mathcal{S} = \{\pi_1, ..., \pi_s\}$ whose square divides the discriminant $d(S)$ of the equation order $S = R_0[\alpha]$ we still need to merge these overorders to obtain the maximal order o_E of E. Without loss of generality we assume that $S \subseteq S_\pi$ for all $\pi \in \mathcal{S}$. We note that the calculation of S_{π_j} $(1 \le j \le s)$ yields R_0-bases $\tau_{j,1}, ..., \tau_{j,n}$ via transformation matrices $T_j \in R_0^{n\times n}$ subject to

$$(1, \alpha, ..., \alpha^{n-1}) = (\tau_{j,1}, ..., \tau_{j,n})\, T_j \ \ .$$

The basis of S_{π_j} is chosen such that $T_j = (t_{\mu\nu}^{(j)})$ is an upper triangular matrix in row reduced Hermite Normal Form. Because of $(S_{\pi_j} : S) = \det(T_j)$ being a power of π_j, say

$$(S_{\pi_j} : S) := \pi_j^{\kappa_j} \ \ ,$$

the diagonal elements of T_j are powers of π_j, too. Since with each element x also αx is in S_{π_j} we conclude that

$$t_{\mu\mu}^{(j)} \mid t_{\mu+1,\mu+1}^{(j)} \ \ (1 \le \mu < n) \ \ ,$$

respectively, for

$$t_{\mu\mu}^{(j)} = \pi_j^{\lambda_\mu^{(j)}}$$

we have

$$\lambda_1^{(j)} \le \lambda_2^{(j)} \le \cdots \lambda_n^{(j)} \ \ .$$

We note that $\prod_{\mu=1}^n \pi_j^{\lambda_\mu^{(j)}} = \pi_j^{\kappa_j}$. Because of $S_{\pi_j} \cap R_0 = S \cap R_0 = R_0$ we also have $\lambda_1^{(j)} = 0$. Setting $T_j^{-1} =: (a_{\mu\nu}^{(j)})$ the basis elements of S_j are given in the form

$$\tau_\mu^{(j)} \ = \ \pi_j^{-\lambda_\mu^{(j)}} \left(\alpha^{\mu-1} + \sum_{k=1}^{\mu-1} a_{k\mu}^{(j)} \alpha^{k-1} \right) \ \ (1 \le \mu \le n\,;\ a_{\mu k}^{(j)} \in R_0) \ \ .$$

We put

$$c_\mu := \prod_{j=1}^{s} \pi_j^{\lambda_\mu^{(j)}}$$

and

$$c_\mu^{(j)} := c_\mu / \pi_j^{\lambda_\mu^{(j)}} \ \ (1 \le j \le s) \ \ .$$

Similarly to a proof of the Chinese remainder theorem we determine elements $d_\mu^{(j)}$ in R_0 subject to

$$1 \;=\; \sum_{j=1}^{s} c_\mu^{(j)} d_\mu^{(j)} \quad .$$

We claim that the elements

$$\omega_\mu \;:=\; \sum_{j=1}^{s} d_\mu^{(j)} \tau_\mu^{(j)} \;\; (1 \le \mu \le n)$$

form an R_0-basis of o_E. Clearly, they belong to o_E. It therefore suffices to show that any element x of o_E has a presentation

$$x \;=\; \sum_{\nu=1}^{n} x_\nu \omega_\nu \;\; (x_\nu \in R_0) \quad .$$

For this we assume that x belongs to $o_E \cap \sum_{\nu=1}^{\mu} F_0 \alpha^{\nu-1}$ for a fixed integer $\mu \in \{1, ..., n\}$ and show that upon subtracting a suitable multiple of ω_μ yields an element of $o_E \cap \sum_{\nu=1}^{\mu-1} F_0 \alpha^{\nu-1}$. For the coefficient ξ_μ of

$$x \;=\; \sum_{\nu=1}^{\mu} \xi_\nu \alpha^{\nu-1} \;\; (\xi_\nu \in F_0)$$

we know that $c_\mu \xi_\mu \in R_0$. Then we get

$$\begin{aligned} x - c_\mu \xi_\mu \omega_\mu \;&=\; x - c_\mu \xi_\mu \sum_{j=1}^{s} d_\mu^{(j)} \tau_\mu^{(j)} \\ &=\; x - c_\mu \xi_\mu \sum_{j=1}^{s} d_\mu^{(j)} \frac{c_\mu^{(j)}}{c_\mu} \left(\alpha^{\mu-1} + \sum_{k=1}^{\mu-1} a_{k\mu}^{(j)} \alpha^{k-1} \right) \\ &=\; x - c_\mu \xi_\mu \frac{1}{c_\mu} \alpha^{\mu-1} - y \quad , \end{aligned}$$

and the element y clearly belongs to $o_E \cap \sum_{\nu=1}^{\mu-1} F_0 \alpha^{\nu-1}$. Hence, the elements $\omega_1, ..., \omega_n$ are indeed an R_0-basis of o_E.

Remark The first basis element ω_1 becomes 1 by this construction.

Example In the example previously discussed the equation order was not maximal for the primes $\pi_1 = 3$ and $\pi_2 = 5$. For the π_j-maximal overorders we obtained bases $1, \alpha, \frac{\alpha^2+\alpha}{3}$ and $1, \alpha, \frac{\alpha^2-2\alpha+1}{5}$, respectively. From this we get $c_1 = c_2 = 1$, $c_3 = 15$. It is easily seen that ω_1 is 1 and that ω_2 is α. To obtain ω_3 we calculate $c_3^{(1)} = 5$, $c_3^{(2)} = 3$ and

$d_3^{(1)} = -1$, $d_3^{(2)} = 2$ and finally

$$\begin{aligned} \omega_3 &= -\frac{\alpha^2+\alpha}{3} + 2\frac{\alpha^2-2\alpha+1}{5} \\ &= \frac{\alpha^2+-17\alpha+6}{15} \quad . \end{aligned}$$

We note that the coefficient of α in the representation of ω_3 can be modified (by adding ω_2) to -2.