Problem 1

Show that the ring $\mathbb{Z}[\sqrt{-2}]$ is Euclidean with respect to the norm map $N(a + b\sqrt{-2}) = a^2 + 2b^2$ $(a, b \in \mathbb{Z})$.

Solution:

We have a norm N:

$$N(a + b\sqrt{-2}) = a^2 + 2b^2 = |a + b\sqrt{-2}|^2, \quad (a, b \in \mathbb{Z}).$$

We want to show, that N is Euclidean norm, i.e.

1. $N(0) = 0$;
2. $a \mid b$ implies $N(a) \leq N(b)$;
3. $(\forall a, b; b \neq 0)(\exists q, r)$: $a = bq + r$, $N(r) < N(b)$.

We can extend N to a function $N : \mathbb{Q}[\sqrt{-2}] \to \mathbb{Q}$ defined similarly by

$$N(a + b\sqrt{-2}) = a^2 + 2b^2 = |a + b\sqrt{-2}|^2, \quad (a, b \in \mathbb{Q}).$$

The condition (1) is trivial, $N(0 + 0\sqrt{-2}) = 0$.

Given any $a + b\sqrt{-2}$, $c + d\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}]$, we have

$$\begin{aligned} N((a + b\sqrt{-2})(c + d\sqrt{-2})) &= N(ac - 2bd + (ad + bc)\sqrt{-2}) = \\ &= (ac - 2bd)^2 + 2(ad + bc)^2 = \\ &= a^2c^2 - 4abcd + 4b^2d^2 + 2a^2d^2 + 4abcd + 2b^2c^2 \\ &= (a^2 + 2b^2)(c^2 + 2d^2) = \\ &= N(a + b\sqrt{-2})N(c + d\sqrt{-2}) \end{aligned}$$

This solves the condition (2) since if $a \mid b$, then $\exists c$: $b = a \cdot c$. And thus $N(b) = N(a \cdot c) = N(a)N(c) \geq N(a)$.

Now, suppose we are given $a + b\sqrt{-2}$, $c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ with $c + d\sqrt{-2} \neq 0$.

Then

$$\begin{aligned}\frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} &= \frac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{c^2+2d^2} = \\ &= \frac{ac-2bd}{c^2+2d^2} + \frac{(ad+bc)}{c^2+2d^2}\sqrt{-2} = \\ &= e+f\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}].\end{aligned}$$

Pick $g, h \in \mathbb{Z}$ such that $|e-g|$, $|f-h| \leq 1/2$ and set

$$\begin{aligned}q &= g+h\sqrt{-2} \\ r &= a+b\sqrt{-2}-q(c+d\sqrt{-2})\end{aligned}$$

Then $a+b\sqrt{-2} = q(c+d\sqrt{-2})+r$ and

$$\begin{aligned}N(r) &= N\left((c+d\sqrt{-2})((e-g)+(f-h)\sqrt{-2})\right) \\ &= N(c+d\sqrt{-2})N((e-g)+(f-h)\sqrt{-2}) \\ &\leq 3/4N(c+d\sqrt{-2}) \\ &< N(c+d\sqrt{-2}).\end{aligned}$$

□

Problem 2

Show that the only solutions $X, Y \in \mathbb{Z}$ of the equation $X^2 + 2 = Y^3$ are $X = \pm 5$ and $Y = 3$.

Solution:

Indeed, $X = \pm 5$ and $Y = 3$ is a solution of given equation. Let $X, Y \in \mathbb{Z}$ be now arbitrary solution.

Claim 1 *Both X and Y are odd.*

First observe, that X and Y are either both odd or both even. If X is even (odd), then X^2 is even (odd), $X^2 + 2 = Y^3$ is even (odd) and therefore Y is also even (odd). Futhermore assume that both are even and look at congruences modulo 4. X can be written as $4k$ or $4k + 2$ for some $k \in \mathbb{Z}$, $X^2 + 2$ is then $16k^2 + 2$ or $16k^2 + 16k + 4 + 2$ which is mod 4 always 2. Y can similarily be written as 4ℓ or $4\ell + 2$ for some $\ell \in \mathbb{Z}$. Y^3 is $64\ell^3$ or $64\ell^3 + 96\ell^2 + 48\ell + 8$, which is mod 4 always 0. We conclude, that X, Y cannot be even and must therefore be odd.

Claim 2 *We can factor $X^2 + 2$ on $\mathbb{Z}[\sqrt{-2}]$ as $(X - \sqrt{-2})(X + \sqrt{-2})$ and the factors are relatively prime.*

By exercise 1.E, $\mathbb{Z}[\sqrt{-2}]$ is an Euclidean ring. It is therefore a principlal ideal ring and hence an unique factorization domain.

We can factor $X^2 + 2 = Y^3$ on $\mathbb{Z}[\sqrt{-2}]$ as

$$(X - i\sqrt{2})(X + i\sqrt{2}) = Y^3.$$

Because gcd of two elements also divides their difference, notice that

$$\gcd(X + \sqrt{-2}, X - \sqrt{-2}) \mid 2\sqrt{-2}.$$

Common divisor also divides the odd number Y^3 and hence $\gcd(X^3, 2)$. Anyway, if $(X - \sqrt{-2})$ and $(X + \sqrt{-2})$ would not be relatively prime, any divisor would have even norm, which is not possible. We conclude that $(X - \sqrt{-2})$ and $(X + \sqrt{-2})$ are relatively prime.

Claim 3 *The only units of $\mathbb{Z}[\sqrt{-2}]$ are 1 and -1. More generaly, let B^* be the group of units of B. For any element x from B holds that $x \in B^*$ if and only if $N(x) = \pm 1$.*

If $xx^{-1} = 1$ then $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$ and hence integer $N(x)$ must be equal to ± 1. On the other hand, if $N(x) = \pm 1$ then the characteristic equation of x has the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1 = 0$, $a_i \in \mathbb{Z}$. Thus $x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2 + a_1) = \mp 1$.

Let us demonstrate the lemma on $\mathbb{Z}[\sqrt{-2}]$: $N(a + b\sqrt{-2}) = a^2 + 2b^2 = \pm 1$. Since $a, b \in \mathbb{Z}$, the only solution is $b = 0$, $a = \pm 1$.

Claim 4 *The only solutions $X, Y \in \mathbb{Z}$ of the equation $X^2 + 2 = Y^3$ are $X = \pm 5$ and $Y = 3$.*

It follows from UFD (generalization of Lemma 1.2.) and the fact about units that for some $Z \in \mathbb{Z}[\sqrt{-2}]$ holds:

$$X + \sqrt{-2} = Z^3 \quad \text{or} \quad Z^3\sqrt{-2} \quad \text{or} \quad Z^3(-2).$$

Taking complex conjugates, we then have

$$X - \sqrt{-2} = W^3 \quad \text{or} \quad W^3\sqrt{-2} \quad \text{or} \quad W^3(-2),$$

where W is the conjugate of Z. Hence, multiplying these together,

$$Y^3 = X^2 + 2 = (Z \cdot W)^3 \quad \text{or} \quad -2(Z \cdot W)^3 \quad \text{or} \quad 4(Z \cdot W)^3.$$

Since $W \cdot Z \in \mathbb{Z}$, unique factorization in $\mathbb{Z}$ implies that

$$X^2 + 2 = (Z \cdot W)^3,$$

and

$$\begin{aligned} X + \sqrt{-2} &= Z^3 \\ X - \sqrt{-2} &= W^3 \end{aligned}$$

Now let $Z = U + V\sqrt{-2}$, $U, V \in \mathbb{Z}$. Then $W = U - V\sqrt{-2}$, and

$$\begin{aligned} X + \sqrt{-2} &= U^3 + 3U^2V\sqrt{-2} - 6UV^2 - 2V^3\sqrt{-2} \\ X - \sqrt{-2} &= U^3 - 3U^2V\sqrt{-2} - 6UV^2 + 2V^3\sqrt{-2} \end{aligned}$$

This implies that $V = 1$ or $V = -1$, and that the only solutions are $V = 1$, $U = 1$ or -1. Then $Y = Z \cdot W = 3$, $X = U^3 - 6UV^2 = \pm 5$.

□

Problem 3

Let $\zeta_5 \in \mathbb{C}$ be a primitive 5-th root of unity. Let $F := \mathbb{Q}(\zeta_5, \sqrt[4]{5})$.

(i) Show that $[F : \mathbb{Q}] = 8$.

Solution:

Claim 5 *The polynomial $\Phi_d(T)$ is of degree $\varphi(d)$, where φ is Euler's phi function.*

This is immediate consenquence of definition: for any positive integer d, we define $\Phi_n(T)$, the d-th cyclotomic polynomial, by

$$\Phi_d(T) = \prod_{j=1,(j,d)=1}^{d} (T - \zeta_d^j),$$

where $\zeta_d = \exp(2\pi i/d)$, i.e. an d-th root of unity. Therefore the degree is $\varphi(d)$.

To move on: Denote $\alpha = \zeta_5$, $\beta = \sqrt[4]{5}$.

Let

$$f(T) = f_{\min}^{\alpha} = \frac{T^5 - 1}{T - 1} = T^4 + T^3 + T^2 + T + 1.$$

be the minimum polynomial of α over $\mathbb{Q}$. By example 2.K.(ii), it is the cyclotomic polynomial $\Phi_5(T)$ with zeroes $\alpha = \alpha_1$, α_2, α_3, α_4 in $\mathbb{C}$. The Eisenstein's criterion (and Prop 2.8.) proves that p-th cyclotomic polynomial $\Phi_p(x)$ is ireducible of degree $\varphi(p) = p - 1$.

Hence and also by the claim,

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 5 - 1 = 4$$

It means, that any field K intermediate between $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}$ must be quadratic over $\mathbb{Q}$.

Divide

$$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$$

by ζ_5^2 and get

$$\zeta_5^2 + \zeta_5 + 1 + \zeta_5^{-1} + \zeta_5^{-2} = \left(\zeta_5 + \frac{1}{\zeta_5}\right)^2 + \left(\zeta_5 + \frac{1}{\zeta_5}\right) - 1 = 0.$$

Solving the quadratic equation, we get that

$$\zeta_5 + \frac{1}{\zeta_5} = \frac{-1 \pm \sqrt{5}}{2}.$$

From the standard picture of 5-th roots of unity in the complex plane, we have that

$$\zeta_5 + \frac{1}{\zeta_5} = e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos\frac{2\pi}{5}.$$

Therefore

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

And we have proved that $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$. In fact, there are no other intermediate fields between $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}$, which is stated in Example 4.4.(i).

Let similarily

$$g(T) = g^{\beta}_{\min} = T^4 - 5$$

be the minimum polynomial of β over $\mathbb{Q}$. Denode $\beta = \beta_1 = \sqrt[4]{5}, \beta_2 = -\sqrt[4]{5}, \beta_3 = i\sqrt[4]{5}, \beta_4 = -i\sqrt[4]{5}$ zeroes of g in $\mathbb{C}$. From Eisenstein criterium, $g(T)$ is also ireducible. Thus $\mathbb{Q}(\sqrt[4]{5})$ is of degree 4.

We will now use the theorem saying that if $T \leq S \leq U$ are extension of fields, then $[U : T] = [U : S] \cdot [S : T]$. We have shown that $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. We want to show that $[\mathbb{Q}(\zeta_5, \sqrt[4]{5}) : \mathbb{Q}(\zeta_5)] = 2$. Thus $[\mathbb{Q}(\zeta_5, \sqrt[4]{5}) : \mathbb{Q}] = 4 \cdot 2 = 8$ We claim that $\sqrt[4]{5} \notin \mathbb{Q}(\zeta_5)$. The polynomial $T^2 - \sqrt{5}$ has, according to what was shown, coefficients in $\mathbb{Q}(\zeta_5)$, is irreducible and his root is $\sqrt[4]{5}$. Thus is a minimal polynomial of $\sqrt[4]{5}$. We conclude that the degree of the extension is the degree of this polynomial which solves the exercise.

□

(ii) Find a primitive element of F.

Solution:

Theorem 2.2. says, that there exists $\theta \in F$ such that $F = \mathbb{Q}(\theta)$. The proof of the theorem gives a way, how to find such element: $\alpha + \lambda\beta$, $\lambda \in \mathbb{Q}$ is a primitive element if $\alpha + \lambda\beta \neq \alpha_i + \lambda\beta_j$ for $1 \leq i \leq 4$ and $2 \leq j \leq 4$. This is clearly true for e.g. $\lambda = 1$. Put thus

$$\theta = \alpha + \beta.$$

It now holds that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$, because $\theta \in \mathbb{Q}(\alpha, \beta)$. To see that $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$, consider polynomial $g(T), \tilde{f}(T) = f(\theta - \lambda T)$. These polynomials are polynomials over the field $F(\theta)$. It is easy to see that these polynomials have one and only one general root $\beta = \beta_1$. Hence their highest common divisor is equal to $(T - \beta_1)$. On the other hand general common divisor

is polynomial in $\mathbb{Q}(\theta)[T]$. Hence $\beta \in \mathbb{Q}(\theta)$ and obviously $\alpha = \theta + \lambda\beta \in \mathbb{Q}(\theta)$. Hence $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$.

□

(iii) Determine r_1 and r_2.

Solution: By exercise 2.j., we know that if $r_1 \geq 1$ then the only roots of unity in F are ± 1. This is not true in this case as ζ_5 is part of this field. We conclude, that $r_1 = 0$ and because $r_1 + 2r_2 = 8$, we have that $r_2 = 4$.

□

Problem 4

Let $f := T^3 - 3T + 9 \in \mathbb{Q}[T]$ and define $F := \mathbb{Q}[T]/(f)$. Write $\alpha \in F$ for the class of T modulo (f). You may assume without proof that f is irreducible in $\mathbb{Q}[T]$, so that F is a field with $[F : \mathbb{Q}] = 3$.

(i) Compute $\mathsf{Disc}(f)$.

Solution:

$$\begin{aligned} f(T) &= T^3 - 3T + 9 \\ f'(T) &= 3T^2 - 3 \end{aligned}$$

By [1, prop. 3.5] is

$$\mathsf{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \cdot \mathsf{Res}(f, f'), \tag{1}$$

where $n = \deg f$. Remains to compute $\mathsf{Res}(f, f')$. We will show twoo different way, how approach the result:

Lemma 6 *If $A(X) = \sum_{0 \le i \le m} a_i X^i$ and $B(X) = \sum_{0 \le i \le n} b_i X^i$, then the resultant $\mathsf{Res}(A, B)$ is equal to the determinant of the Sylvester's $(n+m) \times (n+m)$ matrix (coefficients of A are repeated on n rows, coefficients of B are repeated on m rows).*

The proof is long and rather technical and can be found for instance in A Course In Computational Algebraic Number Theory by Henri Conhen, p. 119.

$$\begin{aligned} \mathsf{Res}(f, f') &= \mathsf{Res}(T^3 - 3T + 9, 3T^2 - 3) = \\ &= \begin{vmatrix} 1 & 0 & -3 & 9 & 0 \\ 0 & 1 & 0 & -3 & 9 \\ 3 & 0 & -3 & 0 & 0 \\ 0 & 3 & 0 & -3 & 0 \\ 0 & 0 & 3 & 0 & -3 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -3 & 9 & 0 \\ 0 & 1 & 0 & -3 & 9 \\ 0 & 0 & 6 & -27 & 0 \\ 0 & 0 & 0 & 6 & -27 \\ 0 & 0 & 0 & 27/2 & -3 \end{vmatrix} = \\ &= \begin{vmatrix} 1 & 0 & -3 & 9 & 0 \\ 0 & 1 & 0 & -3 & 9 \\ 0 & 0 & 6 & -27 & 0 \\ 0 & 0 & 0 & 6 & -27 \\ 0 & 0 & 0 & 0 & 693/12 \end{vmatrix} = 2079 \end{aligned}$$

Second way of computing $\mathsf{Res}(f, f')$ is using exercise 3K(ii).

Lemma 7 *Let K be a field and let $\alpha_1, \ldots, \alpha_r \in K$. Put $g = b\prod_{i=1}^{r}(T-\alpha_i)$ and let $h \in K[T]$ be non-zero polynomial of degree s. Then $\mathsf{Res}(g,h) = b^s \prod_{\alpha, g(\alpha)=0} h(\alpha)$.*

In this case $f = 3(x+1)(x-1)$, $b = 3$, $f' = T^3 - 3T + 9$, $s = \deg f' = 3$. 3K(ii) says, that $\mathsf{Res}(f, f') = b^s f'(1)f'(-1) = 3^3 \cdot 7 \cdot 11 = 2079$.

Pluging the result of $\mathsf{Res}(f, f')$ into equation (1), one gets the result

$$\mathsf{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \cdot \mathsf{Res}(f, f') = (-1)^3 \cdot 2079 = -2079$$

□

(ii) Show that $1, \alpha, \alpha^2$ is not an integral basis for O_F.

Solution:

To show that $(1, \alpha, \alpha^2)$ is not an integral basis, we want to find an integral element z which is not in $\mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z}$. The algorithm introduced in the appendix of chapter 4 and the proof of its correctnes (+ Cor. 7.3.) gives a method, how to find such element.

We have show in 3(i) that $\mathsf{Disc}(f) = \Delta(1, \alpha, \alpha^2) = -2079$. The calculations and the previous equation is based on prop. 3.5. Futhermore, because $-2079 = (-1) \cdot 3^2 \cdot 11 \cdot 21$, the only prime number p with $p^2 \mid \mathsf{Disc}(f)$ is $p = 3$.

We will now look for linear combinations

$$y = a_0 + a_1\alpha + a_2\alpha^2,$$

where $a_i \in \{0, 1, 2 = p-1\}$, $(a_0, a_1, a_1) \neq (0,0,0)$ with the property that y/p is integral.

Put a_0, $a_1 = 0$, $a_2 = 1$ and thus $y = \alpha^2$ and compute:

$$\begin{aligned}\left(\frac{\alpha^2}{3}\right)^2 &= \frac{\alpha^4}{9} = \frac{\alpha^2 - 3\alpha}{3} \\ \left(\frac{\alpha^2}{3}\right)^3 &= \frac{\alpha^6}{27} = \frac{9\alpha^2 - 54\alpha + 81}{27} = \frac{\alpha^2 - 6\alpha + 9}{3}.\end{aligned}$$

To check that $y/3$ is an integral element, we will find a monic polynomial $m(T) \in \mathbb{Z}[T]$ with $m(y/3)$ is 0. Assume that the polynomial exists, then also exists $B, C, D \in \mathbb{Z}$ such that

$$\left(\frac{\alpha^2}{3}\right)^3 + B\left(\frac{\alpha^2}{3}\right)^2 + C\left(\frac{\alpha^2}{3}\right) + 3D = 0.$$

Thus

$$\begin{aligned} 1+B-C &= 0 \\ -6-3B &= 0 \\ 9+3D &= 0 \end{aligned}$$

and one can check, that these equations have solutions $(B, C, D) = (2, -1, -3)$.

Thus $y/3 = (\alpha^2)/3$ is an integral element, since it is a root of polynomial $T^3 + 2T^2 - T - 3$. Futhermore, based on the correctnes of the algorithm and underlying theory in the chapter, $z = y/3$ is not in $\mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z}$.

We have thus found an integral element from O_F that is not in $1\mathbb{Z}+\alpha\mathbb{Z}+\alpha^2\mathbb{Z}$ and we conclude that $(1, \alpha, \alpha^2)$ cannot be an integral basis for O_F.

□

(iii) Give an integral basis and compute Δ_F.

Solution: We will continue using means of the algorithm introduced in the appendix of chapter 4 [Proof Cor. 7.3].

Part 3(ii) has produced a prime number $p = 3$ such that p^2 divides $\Delta(1, \alpha, \alpha^2) = -2079$ and integers $a_0 = 0$, $a_1 = 0$, $a_2 = 1$ such that y/p is integral, where $y = a_0 + a_1\alpha + a_2\alpha^2 = \alpha^2/3$. Acording to the algorithm, we will choose a new basis $(\omega_1, \omega_2, \omega_3) = (1, \alpha, y/p)$. Prop. 3.4(ii) gives, that

$$\Delta\left(1, \alpha, \alpha^2/3\right) = \frac{1}{p^2} \cdot \Delta(1, \alpha, \alpha^2) = -231.$$

Since our new basis is squarefree, prop 4.8 tells us, that it is an integral basis and that $\Delta_F = -231$. That concludes the exercise.

□

Problem 5

Let $f : \mathbb{Z}^3 \to \mathbb{Z}^4$ be the homomorphism given by the matrix

$$\begin{pmatrix} -1 & 1 & 7 \\ -3 & -1 & -3 \\ 0 & 12 & 0 \\ 1 & 11 & 5 \end{pmatrix}.$$

Determine the integers $r \geq 0$ and $a_1, ..., a_t$ with $a_1|a_2|...|a_t$ such that

$$\mathbb{Z}^4/\mathsf{Im}(f) \cong \mathbb{Z}^r \times (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_t\mathbb{Z}).$$

Solution:

Crutial here are Corollary 7.2. and the proof of Theorem 7.1.

Let $G = \mathbb{Z}^4$, $A = \mathbb{Z}^4/(f)$. Let $[t] \in A$ denote a factor class reprezented by the element $t \in \mathbb{Z}^4$. A map $\theta : t \mapsto [t]$ is a surjective map $\mathbb{Z}^4 \to A$. Denote $H_1 = \ker(\theta) = \{t;\, \theta(t) = [t] = [0]\}$, i.e. $H = (f)$.

By Theorem 7.1., there is a basis $e_1, ..., e_4$ of $\mathbb{Z}^4$ and there exist positive integers $a_1|a_2|...|a_m$ such that $a_1e_1, ..., a_me_m$ is a basis for H (in our case $m = 3$).

Then

$$A \cong \mathbb{Z}^{n-m} \times \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z}.$$

The algorithm that follows from the proof of Theorem 7.1. does in the step i the following:

1. $S_i := \{\varphi(h) \mid \varphi \in \mathsf{Hom}(G_i, \mathbb{Z}),\, h \in H_i\}$;
2. $a_i := \mathsf{min}_{a_i>0} S_i$;
3. find $h_i \in H_i$, $\psi_i \in \mathsf{Hom}(G_i, \mathbb{Z})$ such that $\psi_i(h_i) = a_i$;
4. $e_i := a_i^{-1} h_i$;
5. $G_{i+1} := \ker(\psi_i)$, $H_{i+1} := \ker(\psi_i) \cap H$.

In the step $i = 1$, we have $G_1 = G$, $H_1 = H$, $a_1 = 1$, $h_1 = f(1\ 0\ 0) = (-1\ -3\ 0\ 1)$, ψ_1 is defined by the matrix $(-1\ 0\ 0\ 0)$, $e_1 = (-1\ -3\ 0\ 1)$. $G_2 = (0\ k_1\ k_2\ k_3)$, $k_1, k_2, k_3 \in \mathbb{Z}$. $H_2 = (f) \cap G_2$.

$$\begin{aligned} (f) &= \langle(-1\ -3\ 0\ 1), (1\ -1\ 12\ 11), (7\ -3\ 0\ 5)\rangle \\ G_2 &= \langle(0\ 1\ 0\ 0), (0\ 0\ 1\ 0), (0\ 0\ 0\ 1)\rangle\,, \end{aligned}$$

and thus every element k in $(f) \cap G_2$ satisfies the following

$$\begin{aligned} k &= a(-1\ -3\ 0\ 1) + b(1\ -1\ 12\ 11) + c(7\ -3\ 0\ 5) \quad a, b, c \in \mathbb{Z} \\ k &= x(0\ 1\ 0\ 0) + y(0\ 0\ 1\ 0) + z(0\ 0\ 0\ 1) \quad x, y, z \in \mathbb{Z}. \end{aligned}$$

By solving a standard system of linear equations, we have that

$$(a, b, c, x, y, z) = \langle(1\ 1\ 0\ -1\ 12\ 11), (7\ 0\ 1\ -24\ 0\ 12)\rangle$$

and thus

$$H_2 = \langle h_{21} = (0\ -4\ 12\ 12), h_{22} = (0\ -24\ 0\ 12)\rangle\,.$$

Next time, we will skip this basic linear algebra and just give the results.

In the step $i = 2$, we put $a_2 = 4$. Clearly this element is minimal in the set S_2, but let us show a proof. Since each element h_2 in H_2 is of the form $h_2 = \varsigma_1 h_{21} + \varsigma_2 h_{22} = \varsigma_1 4(0\ -1\ 3\ 3) + \varsigma_2 4(0\ -6\ 0\ 2)$, its image under any homomorphism must be divisible by four. That's why a_2 must be divisible by 4 and thus cannot be smaller than 4. Consequently, $h_2 = (0\ -4\ 12\ 12)$, ψ_2 is defined by the matrix $(0\ -1\ 0\ 0)$, $e_2 = (0\ -1\ 3\ 3)$. $G_3 = (k_1\ 0\ k_2\ k_3)$, $k_1, k_2, k_3 \in \mathbb{Z}$. $H_3 = H_2 \cap G_3 = \langle 0\ 0\ 72\ 60 \rangle$.

In the step $i = 3$, $a_3 = 12$ (the argument of minimality is the same as in previous step), $h_3 = (0\ 0\ 72\ 60)$, ψ_3 is defined by the matrix $(0\ 0\ 1\ -1)$, $e_3 = (0\ 0\ 6\ 5)$. $G_4 = (k_1\ k_2\ k_3\ 0)$, $k_1, k_2, k_3 \in \mathbb{Z}$. $H_4 = H_3 \cap G_4 = (0\ 0\ 0\ 0)$. And we have found all we wanted.

The answer is that

$$A \cong \mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

□

Problem 6

Let $f := t^3 + 3t + 3 \in \mathbb{Q}[t]$. Let $F := \mathbb{Q}[t]/(f)$, and write $\alpha \in F$ for the class of t modulo (f). You may use without proof that f is irreducible in $\mathbb{Q}[t]$.

Intermezzo

We will start the solution by a few lines of PARI/GP program. This will give us some view of the result we should expect.

```
gp > poly = x^3 + 3*x + 3 ;
gp > nf = nfinit(poly) ;
gp > nf.disc
%1 = -351
gp > poldisc(nf.pol)
%2 = -351
gp > nf.sign
%3 = [1, 1]
```

```
gp > p2 = idealprimedec(nf, 2)
%4 = [[2, [2, 0, 0]~, 1, 3, [1, 0, 0]~]]
gp > idealnorm(nf, p2[1])
%5 = 8

gp > p3 = idealprimedec(nf, 3)
%6 = [[3, [0, 1, 0]~, 3, 1, [1, 0, 1]~]]
gp > idealnorm(nf, p3[1])
%7 = 3

gp > p5 = idealprimedec(nf, 5)
%8 = [[5, [5, 0, 0]~, 1, 3, [1, 0, 0]~]]
gp > idealnorm(nf, p5[1])
%9 = 125

gp > p7 = idealprimedec(nf, 7)
%10 = [[7, [-1, 1, 0]~, 1, 1, [2, 1, 1]~],
      [7, [-5, 1, 1]~, 1, 2, [-1, 1, 0]~]]
gp > [idealnorm(nf, p7[1]), idealnorm(nf, p7[2])]
%11 = [7, 49]

gp > p11 = idealprimedec(nf, 11)
%12 = [[11, [-5, 1, 0]~, 1, 1, [4, 5, 1]~],
       [11, [2, 1, 0]~, 1, 1, [5, -2, 1]~],
       [11, [3, 1, 0]~, 1, 1, [-1, -3, 1]~]]
gp > [idealnorm(nf,p11[1]), idealnorm(nf,p11[2]), idealnorm(nf,p11[3])]
%13 = [11, 11, 11]

gp > il = ideallist(nf, 11) ;
gp > il[1]
%14 = [[1, 0, 0; 0, 1, 0; 0, 0, 1]]
gp > il[2]
%15 = []
gp > il[3]
%16 = [[3, 0, 1; 0, 1, 0; 0, 0, 1]]
gp > il[4]
%17 = []
gp > il[5]
%18 = []
gp > il[6]
%19 = []
```

```
gp > il[7]
%20 = [[7, 6, 4; 0, 1, 0; 0, 0, 1]]
gp > il[8]
%21 = [[2, 0, 0; 0, 2, 0; 0, 0, 2]]
gp > il[9]
%22 = [[3, 0, 1; 0, 3, 0; 0, 0, 1]]
gp > il[10]
%23 = []
gp > il[11]
%24 = [[11, 6, 6; 0, 1, 0; 0, 0, 1],
       [11, 2, 5; 0, 1, 0; 0, 0, 1],
       [11, 3, 0; 0, 1, 0; 0, 0, 1]]
```

Result 1 gives the answer for problem (i), combined with result 2,3 we have answer for problem (ii) and results 14 to 24 shows all ideals of given norm and thus answers problems (iii) and (iv).

(i) Show that $\mathsf{Disc}(f) = -3^3 \cdot 13$.

Solution:

We will follow example under proposition 4.8. I have shown different approaches how to compute the discriminant in the first assignment.

The characteristic polynomial of α is also equal to $f(T)$. According to the def. 3.3 and prop. 3.5. of the discriminant

$$\mathsf{Disc}(f) = \Delta(1, \alpha, \alpha^2) = \begin{vmatrix} (1) & (\alpha) & (\alpha^2) \\ (\alpha) & (\alpha^2) & (\alpha^3) \\ (\alpha^2) & (\alpha^2) & (\alpha^4) \end{vmatrix}.$$

By definition 3.1., $(x) = \mathsf{Trace}(M_x)$

$$\begin{aligned} (1) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3 \\ (\alpha) &= \begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & -3 \\ 0 & 1 & 0 \end{pmatrix} = 0 \\ (\alpha^2) &= \begin{pmatrix} 0 & -3 & 0 \\ 0 & -3 & -3 \\ 0 & 0 & -3 \end{pmatrix} = -6 \\ (\alpha^3) &= -3(\alpha) - 3(1) = -9 \\ (\alpha^4) &= -3(\alpha^2) - 3(\alpha) = 18 \end{aligned}$$

And thus

$$\mathsf{Disc}(f) = \begin{vmatrix} 3 & 0 & -6 \\ 0 & -6 & -9 \\ -6 & -9 & 18 \end{vmatrix} = -351 = -3^3 \cdot 13.$$

□

(ii) Prove that $O_F = \mathbb{Z}[\alpha]$.

Solution:

First observation is that $f = t^3+3t+3$ is an Eisenstein polynomial for prime $p = 3$. The rest is defined such that we can use prop. 9.3. and conclude that 3 does not divide $[O_F : \mathbb{Z}[\alpha]]$.

By cor. 7.3. and (i), $-3^3 \cdot 13 = \mathsf{Disc}(f) = [O_F : \mathbb{Z}[\alpha]]^2 \cdot \Delta_F$. The only possible choices for $[O_F : \mathbb{Z}[\alpha]]$ are thus 3 and 1. We have negated 3 and thus $[O_F : \mathbb{Z}[\alpha]] = 1$. It follows that $O_F = \mathbb{Z}[\alpha]$.

□

(iii) List all non-zero prime ideals $\mathfrak{p} \subset O_F$ of norm ≤ 11. For each prime ideal in the list you should give explicit generators, and you should give the norm.

Solution:

We will use Factorization Lemma (Th. 9.1.). A prime number p factors in $O_F = \mathbb{Z}[\alpha]$ in the same way as the polynomial $f(T) = T^3 + 3T + 3$ factors in the ring $\mathbb{F}_p[T]$.

Because in $\mathbb{Q}$ is

$$\begin{array}{lll} f(1) = 7 & f(2) = 17 & f(3) = 3 \cdot 13 \\ f(4) = 79 & f(5) = 11 \cdot 13 & f(6) = 79 \cdot 3 \\ f(7) = 367 & f(8) = 11 \cdot 7^2 & f(9) = 3 \cdot 11 \cdot 23 \\ f(10) = 1033 & & \end{array}$$

we see that polynomial $f(T)$ is irreducible modulo 2 and 5. Modulo 3, $f(T) = T^3$; modulo 7, $f(T) = (T-1)(T^2+T-3)$ and modulo 11, $f(T) = (T-5)(T+2)(T+3)$. Thus (2), (5) are primes in O_F with respective norms 8 and 125; $\mathfrak{p}_3 = (\alpha)$ is a prime of norm 3; $(7) = \mathfrak{p}_7\mathfrak{p}_{49}$ where $\mathfrak{p}_7 = (7, \alpha - 1)$ is a prime of norm 7 and $\mathfrak{p}_{49} = (7, \alpha^2+\alpha-3)$ is a prime of norm 49. Finally, $(11) = \mathfrak{p}_{11}\mathfrak{p}'_{11}\mathfrak{p}''_{11}$ where $\mathfrak{p}_{11} = (11, \alpha-5)$, $\mathfrak{p}'_{11} = (11, \alpha+3)$, $\mathfrak{p}''_{11} = (11, \alpha+2)$ are all primes of norm 11.

Answer: there are 6 non-zero prime ideals of norm ≤ 11 in O_F: (2) of norm 8, $\mathfrak{p}_3 = (\alpha)$ of norm 3, $\mathfrak{p}_7 = (7, \alpha - 1)$ of norm 7 and $\mathfrak{p}_{11} = (11, \alpha - 5)$, $\mathfrak{p}'_{11} = (11, \alpha - 8)$, $\mathfrak{p}''_{11} = (11, \alpha - 9)$ all three of norm 11.

□

(iv) How many non-zero ideals $I \subset O_F$ of norm ≤ 11 are there?

Solution:

By 6.1. O_F is a Dedekind ring; 5.2(i) says that every non-zero ideal in O_F is a fractional ideal and Th.5.3. says that every fractional ideal can be written uniquely as a finite product of prime ideals (with exponents in $\mathbb{Z}$). Finally, for non-zero ideals holds (prop. 6.2.) $N(IJ) = N(I)N(J)$. All the neccessary computation was thus done in the part (iii).

The list of ideals:

$$1(O_F),\ (2),\ \mathfrak{p}_3,\ {\mathfrak{p}_3}^2,\ \mathfrak{p}_7,\ \mathfrak{p}_{11},\ \mathfrak{p}'_{11},\ \mathfrak{p}''_{11}.$$

Therefore there are 8 ideals of norm ≤ 11.

□

Problem 7

Let R be a Dedekind ring that has only one maximal ideal. Prove that R is a principal ideal domain.

Solution:

Let $\mathfrak{p}$ be the only one maximal ideal of R. Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\pi R = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of R. If $\mathfrak{a}$ is a proper ideal of R, it is containded in the only maximal ideal $\mathfrak{p}$. But this implies that $\pi \in \mathfrak{p}^2$. We have a contradiction. Hence, $\mathfrak{a}$ equals R and the maximal ideal $\mathfrak{p}$ is a principal ideal and R is a principal ideal domain.

□

Problem 8

(i) If $a \in O_F$, show that a divides $N(a)$ in O_F.

Solution:

Let $f^a_{\mathsf{char}}(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of a over $\mathbb{Q}$ (cf Lemma 4.2(ii)) with $f(a) = 0$. By def. 3.1., $N(a)$ is equal to $(-1)^{\deg F}$ times the constant element of this polynomial. Let $b_1, ..., b_{d-1} \in \mathbb{Z}[T]$ such that

$$f^a_{\mathsf{char}}(T) = T^d + \sum_{i=1}^{d-1} b_i T^i + (-1)^d N(a).$$

Then

$$0 = f^a_{\mathsf{char}}(a) = a^d + \sum_{i=1}^{d-1} b_i a^i + (-1)^d N(a).$$

Thus,

$$a\left(a^{d-1} + \sum_{i=1}^{d-1} b_i a^{i-1}\right) = (-1)^{d+1} N(a).$$

and $N(a)/a = (-1)^{d+1}(a^{d-1} + \sum_{i=1}^{d-1} b_i a^{i-1})$. Because this element is in O_F (O_F is a subring and $a \in O_F$), it follows that a divides $N(a)$.

□

(ii) Prove that $a \in O_F$ is a unit if and only if $N(a) = \pm 1$.

Solution:

If $N(a) = \pm 1$ then let similarly (actually totally identicaly) as in (i) $f^a_{\mathsf{char}}(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of a over $\mathbb{Q}$. By Def. 3.1. the constant coeficient of f^a_{char} must be ± 1. Let $b_1, ..., b_{d-1} \in \mathbb{Z}[T]$ such that

$$f^a_{\mathsf{char}}(T) = T^d + \sum_{i=1}^{d-1} b_i T^i \pm 1.$$

Then

$$a\left(a^{d-1} + \sum_{i=1}^{d-1} b_i a^{i-1}\right) = \pm 1.$$

Since $a^{d-1} + \sum_{i=1}^{d-1} b_i a^{i-1} \in O_F$, it follows that a is a unit in O_F.

Conversely, let a be a unit in O_F. Let $b \in O_F$ with $ab = 1$. Since $N(a)N(b) = N(ab) = N(1) = 1$ and $N(a), N(b) \in \mathbb{Z}$, it follows that $N(a) = \pm 1$.

□

(iii) If $a, b \in O_F$ are associated elements, show that $N(a) = \pm N(b)$. Show, by means of an example, that the converse is not true in general: There exist number fields F and elements $a, b \in O_F$ such that $N(a) = \pm N(b)$ but such that a and b are not associated.

Solution:

If $a, b \in O_F$ are associated elements, there is a unit u with $a = ub$. Because $N(a) = N(ub) = N(u)N(b)$ and due to the fact (ii) that $N(u) = \pm 1$, we have that $N(a) = \pm N(b)$.

For the second part, consider $m = (2 + i)$ and $n = (2 - i)$ in $F = \mathbb{Q}[\sqrt{-1}]$.

$$\begin{aligned} N(m) &= \det(M_{2+i}) = \det \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} = 5 \\ N(n) &= \det(M_{2-i}) = \det \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} = 5 \end{aligned}$$

Thus, both n and m are integral and of the norm 5. Nevertheless,

$$\frac{2+i}{2-i} = \frac{(2+i)^2}{5} = \frac{3}{5} + \frac{4}{5}i$$

which is not a unit of $\mathbb{Q}[\sqrt{-1}]$ and we conclude that m and n are not associated.

□