Solutions 1

1. **a)** Note that $\mathbb{Z}[\frac{\sqrt{5}+1}{2}] = \mathbb{Z}[X]/(X^2-X-1)$ and $\mathbb{F}_4 = \mathbb{F}_2[Y]/(Y^2-Y-1)$. Thus we can define a ring homomorphism $\phi\colon \mathbb{Z}[\frac{\sqrt{5}+1}{2}] \to \mathbb{F}_4$, sending $X = \frac{\sqrt{5}+1}{2}$ to Y. Clearly ϕ is surjective, with kernel (2), so (2) is indeed a maximal ideal, with residue field $\mathbb{F}_4$.

b) The solution is similar to a). Clearly $\mathfrak{p} = \mathfrak{p}'$. Note that $\mathcal{O} = \mathbb{Z}[X]/(X^2+5)$. So we can define a ring homomorphism $\phi\colon \mathcal{O} \to \mathbb{F}_2$, by sending $X = \sqrt{-5}$ to 1. Then ϕ is surjective, with kernel $\mathfrak{p} = \mathfrak{p}'$, so $\mathfrak{p} = \mathfrak{p}'$ is a maximal ideal with residue field $\mathbb{F}_2$.

We can also define a ring homomorphism $\psi\colon \mathcal{O} \to \mathbb{F}_3$, by sending $X = \sqrt{-5}$ to -1. Then ψ is surjective, with kernel $\mathfrak{q}$, so $\mathfrak{q}$ is a maximal ideal with residue field $\mathbb{F}_3$.

c) We define the function $N\colon \mathcal{O} \to \mathbb{Z}_{\geq 0}$, $a + b\sqrt{-5} \mapsto a^2 + 5b^2$. This has the property that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathcal{O}$, and $N(\alpha) = 0$ if and only if $\alpha = 0$, and $N(\alpha) = 1$ if and only if $\alpha = \pm 1$.

Suppose $2 = uv$ for some $u, v \in \mathcal{O}\backslash\{\pm 1\}$, then $N(u)N(v) = N(2) = 4$, so we must have $N(u) = N(v) = 2$. However 2 is not in the image of the function N, contradiction. So 2 is indeed irreducible in $\mathcal{O}$. Similarly, if $1+\sqrt{-5} = uv$, then $N(u)N(v) = N(1+\sqrt{-5}) = 6$, so $\{N(u), N(v)\} = \{2, 3\}$. Since 2 is not in the image of the function N, this is impossible, therefore $1 + \sqrt{-5}$ is irreducible.

$$\begin{aligned}\mathfrak{p}\mathfrak{p}' &= (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) = (4, 2+2\sqrt{-5}, 2+2\sqrt{-5}, 6) = (2),\\ \mathfrak{p}\mathfrak{q} &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5}) =\\ &= (1+\sqrt{-5}).\end{aligned}$$

d) $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, and here 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are all irreducible elements (since $N(2) = 4$, $N(3) = 9$, $N(1 \pm \sqrt{-5}) = 6$, and $2, 3 \notin N(\mathcal{O})$). So the factorization of 6 is not unique, therefore $\mathcal{O}$ is not a unique factorization domain.

Bitte wenden!

e) Let A be a unique factorization domain, and let K be the fraction field of A. Let $\alpha \in K$ be an integral element over A. Then $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$ for some $n \in \mathbb{Z}_{\geq 1}$ and $c_0, \ldots, c_{n-1} \in A$. We can write $\alpha = \frac{u}{v}$ for some $u, v \in A$, where $v \neq 0$, and $\gcd(u, v) = 1$. After multiplying by v^n, we get $u^n + c_{n-1}u^{n-1}v + \cdots + c_0 v^n = 0$. Then $v \mid u^n$, so all prime factors of v are also prime factors of u. However $\gcd(u, v) = 1$, so we v must be a unit in A. So $\alpha \in A$, therefore A is integrally closed in K.

2. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $X^3 - 2$, so we have $[K : \mathbb{Q}] = 3$, and every element of K can be uniquely written in the form $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$, where $a, b, c \in \mathbb{Q}$. So $\mathcal{B}$ is a $\mathbb{Q}$-basis of K. Since $X^3 - 2$ is monic, $\sqrt[3]{2} \in \mathcal{O}_K$, hence $1, \sqrt[3]{2}, \sqrt[3]{2}^2 \in \mathcal{O}_K$. So $\mathbb{Z}1 + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4} \subseteq \mathcal{O}_K$. Now we need to show that if $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathcal{O}_K$ (here $a, b, c \in \mathbb{Q}$), then in fact $a, b, c \in \mathbb{Z}$. Let $\sigma_1, \sigma_2, \sigma_3 \colon K \to \mathbb{C}$ be the embeddings of K into $\mathbb{C}$, where $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_2(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2}$ and $\sigma_3(\sqrt[3]{2}) = \varepsilon^2\sqrt[3]{2}$ (here $\varepsilon = e^{2\pi i/3}$). Since $\alpha \in \mathcal{O}_K$, the images

$$\begin{aligned}
\sigma_1(\alpha) &= a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{C},\\
\sigma_2(\alpha) &= a + b\varepsilon\sqrt[3]{2} + c\varepsilon^2\sqrt[3]{4} \in \mathbb{C},\\
\sigma_3(\alpha) &= a + b\varepsilon^2\sqrt[3]{2} + c\varepsilon\sqrt[3]{4} \in \mathbb{C}
\end{aligned}$$

are also algebraic integers. So the following complex numbers are also algebraic integers:

$$\begin{aligned}
s_1 &= \sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha),\\
s_2 &= \sigma_1(\alpha)\sigma_2(\alpha) + \sigma_1(\alpha)\sigma_3(\alpha) + \sigma_2(\alpha)\sigma_3(\alpha),\\
s_3 &= \sigma_1(\alpha)\sigma_2(\alpha)\sigma_3(\alpha).
\end{aligned}$$

Calculating these expressions (using $\varepsilon^2 = -1 - \varepsilon$), we get that

$$s_1 = 3a, \quad s_2 = 3(a^2 - 2bc), \quad s_3 = a^3 + 2b^3 + 4c^3 - 6abc.$$

These are algebraic integers in $\mathbb{Q}$, hence $s_1, s_2, s_3 \in \mathbb{Z}$. Then $18bc = s_1^2 - 3s_2 \in \mathbb{Z}$, so $27(2b^3 + 4c^3) = 27s_3 - s_1^3 + 3s_1(18bc) \in \mathbb{Z}$. Then

$$\big(27(2b^3 - 4c^3)\big)^2 = \big(27(2b^3 + 4c^3)\big)^2 - 3^6 \cdot 32b^3c^3 = \big(27(2b^3 + 4c^3)\big)^2 - 4(18bc)^3 \in \mathbb{Z},$$

and $27(2b^3 - 4c^3) \in \mathbb{Q}$, so $27(2b^3 - 4c^3) \in \mathbb{Z}$. Hence $4(3b)^3 = 27(2b^3 + 4c^3) + 27(2b^3 - 4c^3) \in \mathbb{Z}$, so $3b \in \mathbb{Z}$. Then $4(3c)^3 = 27(2b^3 + 4c^3) - 2(3b)^3 \in \mathbb{Z}$, thus $3c \in \mathbb{Z}$. So we have $3a, 3b, 3c \in \mathbb{Z}$.

(Remark: another way to get that $3a, 3b, 3c \in \mathbb{Z}$ is to examine the sums $\sigma_1(\alpha) + \varepsilon\sigma_2(\alpha) + \varepsilon^2\sigma_3(\alpha)$ and $\sigma_1(\alpha) + \varepsilon^2\sigma_2(\alpha) + \varepsilon\sigma_3(\alpha)$ instead of s_2 and s_3.)

Siehe nächstes Blatt!

Let $A = 3a$, $B = 3b$, $C = 3c$, then $A, B, C \in \mathbb{Z}$, and $3s_2 = A^2 - 2BC$, $27s_3 = A^3+2B^3+4C^3-6ABC$, so $3 \mid A^2-2BC$ and $27 \mid A^3+2B^3+4C^3-6ABC$. We may add any integer to a, b or c, because $\alpha \in \mathcal{O}_K$ will remain true, since $1, \sqrt[3]{2}, \sqrt[3]{4} \in \mathcal{O}_K$. So without loss of generality, we may assume that $a, b, c \in [-\frac{1}{2}, \frac{1}{2})$. Then $A, B, C \in [-\frac{3}{2}, \frac{3}{2}) \cap \mathbb{Z} = \{-1, 0, 1\}$. So $|A^3+2B^3+4C^3-6ABC| \leq 1+2+4+6 = 13 < 27$, so we must have $A^3 + 2B^3 + 4C^3 - 6ABC = 0$. Then $2 \mid A^3$, so $A = 0$. Hence $B^3 + 2C^3 = 0$, so $2 \mid B^3$, therefore $B = 0$ and $C = 0$. This means that $a = b = c = 0$, so in general $a, b, c \in \mathbb{Z}$, proving that $\mathcal{B}$ is an integral basis for $\mathcal{O}_K$.

The disrciminant of K is $\Delta_K = \det(\sigma_i(\omega_j))^2$, where $\omega_1 = 1$, $\omega_2 = \sqrt[3]{2}$, $\omega_3 = \sqrt[3]{4}$, so

$$\Delta_K = \det \begin{pmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 1 & \varepsilon\sqrt[3]{2} & \varepsilon^2\sqrt[3]{4} \\ 1 & \varepsilon^2\sqrt[3]{2} & \varepsilon\sqrt[3]{4} \end{pmatrix}^2 = \sqrt[3]{2}^2 \cdot \sqrt[3]{4}^2 \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon \end{pmatrix}^2 = 4 \cdot (-27) =$$
$$= -108.$$

The discriminant of a polynomial $f(X) = a_n(X - \alpha_1) \cdots (X - \alpha_n)$ is $\Delta(f) = a_n^{2n-2} \prod_{i<j}(\alpha_i - \alpha_j)^2$. In our case $f(X) = X^3 - 2 = (X - \sqrt[3]{2})(X - \varepsilon\sqrt[3]{2})(X - \varepsilon^2\sqrt[3]{2})$, where $\varepsilon = e^{2\pi i/3}$. So using $\varepsilon^2 = -1 - \varepsilon$, we get that

$$\Delta(f) = \sqrt[3]{2}^6\big((1-\varepsilon)(1-\varepsilon^2)(\varepsilon-\varepsilon^2)\big)^2 = 4\big((1-\varepsilon)(2+\varepsilon)(1+2\varepsilon)\big)^2 =$$
$$= 4\big(3(1+2\varepsilon)\big)^2 = 36(1+2\varepsilon)^2 = -108.$$

(Another way to get $\Delta(f)$ is to calculate the resultant $R(f, f')$ using the Sylvester determinant.) So $\Delta_K = \Delta(f)$.

3. **a)** Let us fix an algebraic closure $\overline{K}$ of K, and let $\mathcal{O}$ denote the ring of those elements of $\overline{K}$ which are integral over A. Since A is integrally closed, we have $K \cap \mathcal{O} = A$.

If $P \in A[X]$, then trivially α is integral over A. Conversely, suppose α is integral over A. Then $Q(\alpha) = 0$ for some monic polynomial $Q \in A[X]$, so $P \mid Q$ in $K[X]$, i.e. $Q = PR$ for some $R \in K[X]$. Let $P(X) = (X - \alpha_1) \cdots (X - \alpha_n)$, where $\alpha_1, \ldots, \alpha_n \in \overline{K}$. Then $Q(\alpha_1) = \cdots = Q(\alpha_n) = 0$, so $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$. The coefficients $a_1, \ldots, a_n$ of $P(X)$ are (up to a ± 1 factor) elementary symmetric polynomials of $\alpha_1, \ldots, \alpha_n$, so they are also in $\mathcal{O}$. Thus $a_1, \ldots, a_n \in K \cap \mathcal{O} = A$, therefore $P \in A[X]$.

b) Since α is integral over A, we know from a) that $P \in A[X]$. First suppose $L = K(\alpha)$. In this case $\mathrm{Tr}_{L/K}(\alpha) = -a_1$ and $\mathrm{Nm}(\alpha) = (-1)^n a_n$, because

Bitte wenden!

$1, \alpha, \ldots, \alpha^{n-1}$ is a basis of L over K, and the K-linear endomorphism $L \xrightarrow{\cdot\alpha} L$ has the following matrix in this basis:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$$

(It is easy to check that the trace and determinant of this matrix is $-a_1$ and $(-1)^n a_n$.) Since $a_1, a_n \in A$, we get that $\mathrm{Nm}_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in A$.

General case: $K \subseteq K(\alpha) \subseteq L$. Let $m = [L : K(\alpha)]$ be the degree of the field extension $L/K(\alpha)$. Then it is well known that $\mathrm{Nm}_{L/K}(\alpha) = \mathrm{Nm}_{K(\alpha)/K}(\alpha)^m$ and $\mathrm{Tr}_{L/K}(\alpha) = m \,\mathrm{Tr}_{K(\alpha)/K}(\alpha)$. We have already seen that $\mathrm{Nm}_{K(\alpha)/K}(\alpha)$ and $\mathrm{Tr}_{K(\alpha)/K}(\alpha)$ are in A, so also $\mathrm{Nm}_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in A$.

c) Let $\alpha \in B$. If α is a unit in B, then $\alpha\beta = 1$ for some $\beta \in B$, hence $\mathrm{Nm}_{L/K}(\alpha)\,\mathrm{Nm}_{L/K}(\beta) = \mathrm{Nm}_{L/K}(1) = 1$. Here $\mathrm{Nm}_{L/K}(\alpha), \mathrm{Nm}_{L/K}(\beta) \in A$ by b), therefore $\mathrm{Nm}_{L/K}(\alpha)$ is a unit in A.

Conversely, suppose $N_{L/K}(\alpha)$ is a unit in A. Then clearly $\alpha \neq 0$. Since $N_{L/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^m$ (where $m = [L : K(\alpha)]$), $N_{K(\alpha)/K}(\alpha) = (-1)^n a_n$ is a also a unit in A. So a_n is a unit in A. We multiply the equation

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$$

by $a_n^{-1}\alpha^{-n}$:

$$(\alpha^{-1})^n + \frac{a_{n-1}}{a_n}(\alpha^{-1})^{n-1} + \cdots + \frac{1}{a_n} = 0.$$

So $\alpha^{-1} \in L$ is integral over A, hence $\alpha^{-1} \in B$, therefore α is a unit in B.

4. a) The $\mathbb{Q}$-bilinearity of β follows from the $\mathbb{Q}$-linearity of $\mathrm{Tr}_{K/\mathbb{Q}}$.

Symmetry: $\beta(\omega, \omega') = \mathrm{Tr}_{K/\mathbb{Q}}(\omega\omega') = \mathrm{Tr}_{K/\mathbb{Q}}(\omega'\omega) = \beta(\omega', \omega)$.

Non-degenerateness: Let $\omega \in K$ such that $\beta(\omega, \omega') = 0$ for every $\omega' \in K$. Suppose $\omega \neq 0$, then for $\omega' = \frac{1}{\omega}$ we get $0 = \beta(\omega, \frac{1}{\omega}) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}] = n \neq 0$. This contradiction shows that ω must be 0.

b) In the lecture we have defined the discriminant $\Delta_K = \det(\sigma_i(\omega_j))^2$, where $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ are the embeddings of K into $\mathbb{C}$. Recall that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{k=1}^{n} \sigma_k(\alpha)$ for every $\alpha \in K$.

Siehe nächstes Blatt!

Let us take the matrix $M = (\sigma_i(\omega_j)) \in \mathbb{C}^{n\times n}$. Then

$$(M^\mathsf{T}M)_{i,j} = \sum_{k=1}^{n} M_{k,i}M_{k,j} = \sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i\omega_j) = \\ = \mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j),$$

so

$$\det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) = \det(M^\mathsf{T}M) = \det(M^\mathsf{T})\det(M) = \det(M)^2 = \\ = \det(\sigma_i(\omega_j))^2 = \Delta_K.$$

Proof of $\Delta_K \in \mathbb{Z}\setminus\{0\}$: Since all the ω_i are in $\mathcal{O}_K$, also $\omega_i\omega_j \in \mathcal{O}_K$, hence by exercise 3b), $\beta(\omega_i,\omega_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j) \in \mathbb{Z}$. Thus $\Delta_K = \det(\beta(\omega_i,\omega_j)) \in \mathbb{Z}$. This determinant is nonzero, because $\omega_1,\ldots,\omega_n$ is a $\mathbb{Q}$-basis of K, and β is non-degenerate.

(In more details: If $\det(\beta(\omega_i,\omega_j)) = 0$, then there is a linear dependence between the rows of the matrix $(\beta(\omega_i,\omega_j))$, so there exists a vector $(c_1,\ldots,c_n) \in \mathbb{Q}^n\setminus\{0\}$ such that $\sum_{i=1}^n c_i\beta(\omega_i,\omega_j) = 0$ for every j. Then $\beta(\sum_{i=1}^n c_i\omega_i,\omega_j) = 0$ for every j, so $\sum_{i=1}^n c_i\omega_i = 0$ by the non-degenerateness of β. Hence $c_1 = \cdots = c_n = 0$, contradiction.)