Solutions 1

Norm, Trace, Discriminant and Rings of Integers

1. Show that $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

   Solution: Because $\mathbb{Q}(i)$ is a quadratic number field with $i^2 + 1 = 0$, a proposition from the lecture tells us that the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. Since $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, \overline{(\cdot)}\}$, where $\overline{(\cdot)}$ denotes complex conjugation, we have

$$\mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$$

   for $\alpha = a + bi \in \mathbb{Z}[i]$. We know from the lecture that α is a unit in $\mathbb{Z}[i]$ if and only if $\mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha)$ is a unit in $\mathbb{Z}$, i.e. ± 1. But the only elements of $\mathbb{Z}[i]$ with norm ± 1 are $\pm 1, \pm i$ and the conclusion follows.

2. Let k be a field of characteristic $\neq 2$. Let $A := k[x]$ for some transcendental x and let $K := k(x)$ denote its fraction field. Let $L := K[y]/(y^2 - f)$ for some separable $f \in A$ with $\deg f > 0$, and let B be the integral closure of A in L. Show that

$$B = A \oplus A \cdot y.$$

   Solution: Since $y^2 - f = 0$, the element y is integral over A and thus $A \oplus A \cdot y \subseteq B$. To show the reverse inclusion, let $\alpha \in B$. We can write $\alpha = a + by$ with $a, b \in K$, because 1 and y form a K-basis of L. We need to show that $a, b \in A$. By a proposition from the lecture, we know that $\mathrm{Tr}_{L/K}(\alpha), \mathrm{Nm}_{L/K}(\alpha) \in A$. Since L is galois of degree 2 over K with the nontrivial automorphism mapping y to $-y$, we obtain

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &= (a + by) + (a - by) = 2a \\ \mathrm{Nm}_{L/K}(\alpha) &= (a + by)(a - by) = a^2 - b^2y^2 = a^2 - b^2 f. \end{aligned}$$

   The number 2 is invertible in $k \subseteq A$ and therefore $a \in A$. Hence $b^2 f \in A$. Because f is separable, it is squarefree and therefore any nonconstant denominator of b^2 cannot divide f. It follows that b^2 does not have a nonconstant denominator and hence $b \in A$, as desired.

3. Determine the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ and its discriminant.

   Solution: This solution partly follows `https://math.stackexchange.com/a/183093`. Let $K := \mathbb{Q}(\sqrt[3]{2})$. We show that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. Let $\alpha = \frac{a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2}{3} \in \mathcal{O}_K \smallsetminus \mathbb{Z}$ be some element. We need to show that the a_i are integers and $\equiv 0 \bmod 3$.

The minimal polynomial p of α has degree 3. By considering the action of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of the Galois closure $L = \mathbb{Q}[\sqrt[3]{2}, e^{2\pi i/3}]$ of K, we see that

$$p = (X - \alpha)(X - \sigma(\alpha))(X - \sigma^2(\alpha))$$

for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ with $\sigma(\sqrt[3]{2}) = e^{2\pi i/3}\sqrt[3]{2}$ and $\sigma(e^{2\pi i/3}) = e^{2\pi i/3}$. After expanding, we obtain

$$p = X^3 - a_1X^2 + \frac{a_1^2 - 2a_2a_3}{3}X + \frac{6a_1a_2a_3 - a_1^3 - 2a_2^3 - 4a_3^3}{27} =: X^3 + e_1X^2 + e_2X + e_3.$$

and the coefficients e_i lie in $\mathbb{Z}$. Hence $a_1 \in \mathbb{Z}$. By a direct calculation, we see that $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}\alpha) = -2a_3$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}^2\alpha) = -2a_2$ and therefore $2a_2, 2a_3 \in \mathbb{Z}$. Consider the equation:

$$27 \cdot 4 \cdot e_3 = 6a_1 \cdot 2a_2 \cdot 2a_3 - 4a_1^3 - 8a_2^3 - 16a_3^3.$$

All summands on the right-hand side are integers and all of them, except possibly $8a_2^3$, are even. It follows that $8a_2^3$ is even and hence $a_2 \in \mathbb{Z}$, because the left-hand side is even. It follows that all of the summands, except possibly $16a_3^3$, are divisible by 4. Hence $16a_3^3$ is divisible by 4 and therefore $a_3 \in \mathbb{Z}$, because the left-hand side is divisible by 4. Thus all of a_1, a_2, a_3 lie in $\mathbb{Z}$.

By adding integer multiples of $1, \sqrt[3]{2}, \sqrt[3]{2}^2$, we may assume that $a_i \in \{-1, 0, 1\}$ for all i. Because $|a_i| \leqslant 1$, the absolute value of the numerator of e_3 is smaller than 27 and hence $e_3 = 0$. This implies, by a case distinction on the values of the a_i, that all of them are zero and therefore $\equiv 0 \bmod 3$, as desired.

To calculate the discriminant, we need to calculate the traces of $1, \sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt[3]{2}^3 = 2$ and $\sqrt[3]{2}^4 = 2\sqrt[3]{2}$. Because the coefficients of X^2 in the minimal polynomials $X^3 - 2$ and $X^3 - 4$ of $\sqrt[3]{2}$ and $\sqrt[3]{2}^2$ vanish, the traces of those two elements also vanish. We calculate

$$\begin{aligned}\mathrm{disc}(\mathcal{O}_K) &= \det\begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}^2) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}^2) & \mathrm{Tr}_{K/\mathbb{Q}}(2) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}^2) & \mathrm{Tr}_{K/\mathbb{Q}}(2) & \mathrm{Tr}_{K/\mathbb{Q}}(2\sqrt[3]{2}) \end{pmatrix} \\ &= \det\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix} = -108 = -2^4 \cdot 3^3.\end{aligned}$$

4. This is an example by Dedekind of a cubic number field K whose ring of integers is not generated by one element over $\mathbb{Z}$.

   (a) Show that the polynomial $f := X^3 + X^2 - 2X + 8$ is irreducible over $\mathbb{Q}$ and thus defines a cubic number field $K := \mathbb{Q}(\theta)$ with $f(\theta) = 0$.

(b) Show that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \theta \oplus \mathbb{Z} \cdot \beta$ for $\beta := \frac{\theta+\theta^2}{2}$.

(c) Show that the kernel of the surjection $\mathbb{Z}[X,Y] \twoheadrightarrow \mathcal{O}_K$ defined by $g(X,Y) \mapsto g(\theta,\beta)$ is the ideal

$$(X^2 - 2Y + X,\ XY - X + 4,\ Y^2 - Y + 2X + 2).$$

(d) Deduce that $\mathcal{O}_K/2\mathcal{O}_K \cong (\mathbb{F}_2)^3$.

(e) Show that $(\mathbb{F}_2)^3$ is not generated by one element over $\mathbb{F}_2$.

(f) Deduce that there exists no $\xi \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\xi]$.

Solution: For a different approach by Brian Conrad to this example see:
`https://math.stanford.edu/~conrad/154Page/handouts/nonprim.pdf`

(a) Since f is primitive over $\mathbb{Z}$ and of positive degree, by the Gauss lemma, the polynomial f is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$. Consider the reduction $\bar{f} = X^3 + X^2 + X + 2 \in \mathbb{F}_3[X]$ of f modulo 3. If f is reducible over $\mathbb{Z}$, then it has a root in $\mathbb{Z}$ and hence the reduction has a root in $\mathbb{F}_3$. Since $\bar{f}$ does not have a root in $\mathbb{F}_3$ the conclusion follows.

(b) The number θ is integral over $\mathbb{Z}$ because its minimal polynomial has integer coefficients. Since $\beta^2 - \beta + 2\theta + 2 = 0$, the number β is integral over $\mathbb{Z}[\theta]$ and hence integral over $\mathbb{Z}$. Furthermore, the numbers $1, \theta, \beta$ are $\mathbb{Z}$-linearly independent, because they are $\mathbb{Q}$-linearly independent. Thus $\mathcal{O}_K$ contains $\Gamma := \mathbb{Z} \oplus \mathbb{Z} \cdot \theta \oplus \mathbb{Z} \cdot \beta$.

To prove equality we compute the discriminant of Γ. We have $\mathrm{Tr}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}] = 3$. To calculate the traces of θ and θ^2, we write down the matrix of the $\mathbb{Q}$-linear map $K \ni x \mapsto \theta x$ with respect to the basis $(1, \theta, \beta)$. It is

$$M := \begin{pmatrix} 0 & 0 & -4 \\ 1 & -1 & 1 \\ 0 & 2 & 0 \end{pmatrix}.$$

We see that $\mathrm{Tr}_{K/\mathbb{Q}}(\theta) = \mathrm{Tr}(M) = -1$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\theta^2) = \mathrm{Tr}(M^2) = 5$. To calculate the traces of $\beta, \theta\beta$ and β^2, we use the $\mathbb{Q}$-linearity of the trace and the relation for θ^3 given by its minimal polynomial. We obtain

$$\begin{aligned} \mathrm{disc}(\Gamma) &= \det \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1) & \mathrm{Tr}_{K/\mathbb{Q}}(\theta) & \mathrm{Tr}_{K/\mathbb{Q}}(\beta) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\theta) & \mathrm{Tr}_{K/\mathbb{Q}}(\theta^2) & \mathrm{Tr}_{K/\mathbb{Q}}(\theta\beta) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\beta) & \mathrm{Tr}_{K/\mathbb{Q}}(\beta\theta) & \mathrm{Tr}_{K/\mathbb{Q}}(\beta^2) \end{pmatrix} = \det \begin{pmatrix} 3 & -1 & 2 \\ -1 & 5 & -13 \\ 2 & -13 & -2 \end{pmatrix} \\ &= -503 \end{aligned}$$

By a proposition from the course we know that

$$\mathrm{disc}(\Gamma) = [\mathcal{O}_K : \Gamma]^2 \, \mathrm{disc}(\mathcal{O}_K).$$

Since 503 is prime and $\mathrm{disc}(\mathcal{O}_K) \in \mathbb{Z}$ it follows that $[\mathcal{O}_K : \Gamma] = 1$ and hence $\Gamma = \mathcal{O}_K$, as desired.

(c) The three generators of the ideal were obtained by expressing $\theta^2, \theta\beta, \beta^2$ in terms of the basis $1, \theta, \beta$. So the ideal I generated by them is contained in the kernel of the surjection. Conversely, by induction on the degree we find that every polynomial in $\mathbb{Z}[X, Y]$ is congruent modulo I to a polynomial of degree $\leqslant 1$. But since $1, \theta, \beta$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, the only polynomial of degree $\leqslant 1$ in the kernel is the zero polynomial. Therefore the kernel is I.

(d) By part (c), we have $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[\bar{X}, \bar{Y}]/\bar{I}$, where $\bar{X}, \bar{Y}, \bar{I}$ are the images of X, Y, I in the reduction. By direct calculation, the homomorphism $\mathbb{F}_2[\bar{X}, \bar{Y}] \to (\mathbb{F}_2)^3$, $f \mapsto (f(1,1), f(0,0), f(0,1))$ vanishes on the generators of $\bar{I}$; hence it induces a homomorphism of $\mathbb{F}_2$-algebras $\mathbb{F}_2[\bar{X}, \bar{Y}]/\bar{I} \to (\mathbb{F}_2)^3$. This homomorphism is surjective, because it comes from the evaluation at three distinct and hence pairwise coprime maximal ideals. On the other hand, part (b) implies that both sides are $\mathbb{F}_2$-vector spaces of dimension 3. Thus the homomorphism is an isomorphism.

(e) Assume, for contradiction, that $(\mathbb{F}_2)^3$ is generated by α over $\mathbb{F}_2$. Then $\alpha^2 = \alpha$, because every element of $\mathbb{F}_2$ satisfies the same equality. Thus $\mathbb{F}_2[\alpha] = \mathbb{F}_2 + \mathbb{F}_2\alpha$ has cardinality $\leqslant 4 < 8 = |(\mathbb{F}_2)^3|$, contradiction.

(f) Assume, for contradiction, that $\mathcal{O}_K = \mathbb{Z}[\xi]$. Then, by part (d), we have $(\mathbb{F}_2)^3 = \mathbb{F}_2[\bar{\xi}]$, where $\bar{\xi}$ is the image of ξ in the reduction. By part (e), this is a contradiction.

5. Two field extensions L/K and L'/K are called *linearly disjoint over* K if $L \otimes_K L'$ is a field. Let $L := \mathbb{Q}(\sqrt[3]{3})$ and let $L' := \mathbb{Q}(\zeta\sqrt[3]{3})$, where ζ is a primitive 3rd root of unity. Show that $L \cap L' = \mathbb{Q}$, but L and L' are not linearly disjoint over $\mathbb{Q}$.

Solution: Let $K = L \cap L'$. We obtain the towers $L/K/\mathbb{Q}$ and $L'/K/\mathbb{Q}$. Because $[L : \mathbb{Q}] = [L' : \mathbb{Q}] = 3$ is prime, it follows from the multiplicativity of the extension degrees that either $L = K = L'$ or $K = \mathbb{Q}$. But $L \neq L'$, because L' contains elements like $\zeta\sqrt[3]{3}$ that lie in $\mathbb{C} \smallsetminus \mathbb{R}$, while $L \subseteq \mathbb{R}$. Hence $L \cap L' = \mathbb{Q}$.

To show that L and L' are not linearly disjoint, we use a proposition from the lecture: The fields L and L' are linearly disjoint if and only if $[LL' : \mathbb{Q}] = [L : \mathbb{Q}] \cdot [L' : \mathbb{Q}]$. We have $LL' = \mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ and $\zeta^2 + \zeta + 1 = 0$ and hence $[LL' : \mathbb{Q}] = 6 < [L : \mathbb{Q}] \cdot [L' : \mathbb{Q}] = 9$. In conclusion, the fields L and L' are not linearly disjoint.

6. Let L/K be an inseparable finite field extension. Then $\mathrm{Tr}_{L/K}$ is identically zero.

Solution: See, for example, Lemma 1.1 in the following notes by Brian Conrad: `https://math.stanford.edu/~conrad/676Page/handouts/normtrace.pdf`