**Algebra 2** **Problem sheet** **Autumn 2022**

NB, every problem is worth 1 credit notwithstanding the difficulty!

**1.** Let $0 \neq \alpha \in \mathbb{Q}[\sqrt[3]{7}]$. Find its reciprocal, that is, $a, b, c \in \mathbb{Q}$ such that $\alpha(a + b\sqrt[3]{7} + c\sqrt[3]{49}) = 1$. During the computation you will get a $3 \times 3$ sytem of equations. What is the determinant? Why is it nonzero?

**2.** Show that if $d \in \mathbb{Z}$ is not a square then $K_d = \mathbb{Q}[\sqrt{d}]$ is a degree 2 field extension. Show that $\mathrm{Gal}(K_d/\mathbb{Q}) \cong Z_2$. Determine when is $K_d = K_e$? Show that for every $\mathbb{Q} \leq E$ degree 2 field extension there exists $d \in \mathbb{Z}$ such that $E = K_d$.

**3.** Suppose $F \leq E$ is a separable extension of *finite* fields. Show that $\exists \alpha \in E$ such that $E = F[\alpha]$.

**4.** Let $\alpha$ be a root of $f(x) = x^3 - 7x + 7$. Determine $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$.

**5.** Let $E$ be a splitting field of $g(x) = x^3 - 7$. Determine $\mathrm{Gal}(E/\mathbb{Q})$ and all the intermediate fields $\mathbb{Q} \leq L \leq E$.

**6.** Suppose $p$ is a prime and $p^2|n$. Show that $\mu(n) = 0$. Also show that if $n = p_1 p_2 \cdots p_k$ is a product of distinct primes then $\mu(n) = (-1)^n$. Conclude that $\mu(ab) = \mu(a)\mu(b)$ is $(a, b) = 1$.

**7.** Suppose $F \leq E \leq \mathbb{C}$ and $F$ contains the $n = |E : F|$-th roots of 1. If $\mathrm{Gal}(E/F)$ is cyclic then there exists $\alpha \in E$ such that $\alpha^n \in F$ and $E = F[\alpha]$. (Hint: You may want to consider a sum $\sum_j \varepsilon_n^j \sigma_j(\zeta)$.)

**8.** *(SOLVED)* Let $R_d$ denote the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$. Determine $R_d$ as a $\mathbb{Z}$-module (up to isomporphism), in particular, when is $R_d = \mathbb{Z}[\sqrt{d}]$?

**9.** For which primes $p$ is $x^2 + x + 1 \in \mathbb{F}_p[x]$ irreducible?

**10.** Let $\alpha = 1 + \sqrt{2} \in R_2$. Show that $\alpha$ is a unit of $R_2$ and there is no unit of $R_2$ in the open interval $(1; \alpha)$. Conclude that every unit $\beta \in R_2$ is of the form $\beta = \pm\alpha^k$, where $k \in \mathbb{Z}$.

**11.** *((i) and (ii) are SOLVED)* Recall that an integral domain is a commutative ring with 1 and without zero-divisors.

(i) Let $R$ be a UFD. Show that $x \in R$ is irreducible if and only if $R/(x)$ is an integral domain and $x \neq 0$.

(ii) Show that every finite integral domain is a field.

(iii) Show that 3 is irreducible in $\mathbb{Z}[\sqrt{5}]$ but $R/(3)$ is not an integral domain.

**12.** We know that the map "evaluation at $i$": $\mathbb{Z}[x] \to \mathbb{Z}[i] = R_{-1}$ is a homomorphism with kernel $(x^2+1)\,\mathbb{Q}[x] \cap \mathbb{Z}[x]$.

(i) Show that $(x^2+1)\,\mathbb{Q}[x] \cap \mathbb{Z}[x] = (x^2+1)\,\mathbb{Z}[x]$ and that the above map induces an isomorphism $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$.

(ii) For any irreducible $\pi \in \mathbb{Z}[i]$ either $\pi|2$ or $\mathbb{Z}[i]/(\pi)$ is a finite field of $N(\pi) = \pi\overline{\pi}$ elements.

(iii) Let $p \in \mathbb{Z}$ be an integer prime. What is $\mathbb{Z}[i]/(p)$ isomoprhic to?

(iv) For which polynomials does (i) generalise?

**13.** What is wrong with the following proof?

Theorem: There are infinitely many irreducible elements of $\mathcal{O}(\mathbb{Q}(\alpha))$.

Proof: Suppose there are finitely many: $\beta_1, \beta_2, \ldots, \beta_k$. Then none of these divide $\gamma = 1 + \prod \beta_j$. But we know that $\gamma$ can be factored into a product of irreducibles and hence all the irreducible divisors of $\gamma$ are new. A contradiction.

**14.** Let $R$ be an integral domain with field of fractions $K$. Let $f(x) = \sum_{i=0}^{m} f_i x^i$ and $g(x) = \sum_{i=0}^{n} g_i x^i$ polynomials from $R[x]$. We define their *resultant*, $\mathrm{Res}(f(x), g(x)) = \det(S)$, where $S$ is an $n+m \times n+m$ matrix with the coefficients of $f(x)$ in the first $n$ rows and the coefficients of $g(x)$ in the last $m$ rows as follows:

$$S = \begin{pmatrix}
f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & 0 & 0 & \cdots & 0 \\
0 & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\
0 & 0 & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 \\
g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\
0 & g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\
0 & 0 & g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & g_n & g_{n-1} & g_{n-2} & \cdots & g_1 & g_0
\end{pmatrix}.$$

Show that $\mathrm{Res}(f(x), g(x)) = 0$ if and only if $(f(x), g(x)) \neq 1$. Furthermore, if $\alpha_i$ are the roots of $f(x)$ and $\beta_j$ are the roots of $g(x)$ in an algebraic closure of $K$ then $\mathrm{Res}(f(x), g(x)) = f_m^n \prod_{i=1}^{m} g(\alpha_i)$.

**15.** Suppose $\alpha \in \mathbb{C}$ has (monic) minimal polynomial $f(x) \in \mathbb{Q}[x]$ of degree $m$. Show that

$$(-1)^{m(m-1)/1} \operatorname{Res}(f, f') = \Delta(1, \alpha, \alpha^2, \ldots, \alpha^{m-1}).$$

This is also called the discriminant of $f(x)$.

**16.** Let $A \leq B$ are rings with fields of fractions $F \leq E$. Suppose $\alpha \in B$ is integer over $A$ with minimal polynomial $f(x) \in A[x]$ and $E$ is its splitting field over $F$. Then the action of $G = \operatorname{Gal}(E/F)$ on the roots of $f(x)$ defines a natural embedding $G \leq S_n$. Prove that $G \leq A_n$ if and only if the discriminant of $f(x)$ is a square in $A$.

**17.** Let $K \geq \mathbb{Q}$ be an algebraic number field, $|K : \mathbb{Q}| = n$ and $\mathcal{O} = \Omega \cap K$ its ring of integers. Suppose $G \leq \mathcal{O}$ is a subgroup of the additive group of $\mathcal{O}$ (in other words, a $\mathbb{Z}$-submodule) with $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Show that

(i) $\Delta_G = \Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ is divisible by $|\mathcal{O}/G|^2$;

(ii) if $G < \mathcal{O}$ then there exists a $p \in \mathbb{Z}$ prime, $p^2 | \Delta_G$ and integers $0 \leq \lambda_i < p$ (not all 0) such that

$$\frac{1}{p}(\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n) \in \mathcal{O}\,.$$

(Such a prime is called *index divisor* and these can be used iteratively to find the integer basis.)

**18.** Let $k, m \in \mathbb{Z}$ with $m \geq 3$ and $(m, k) = 1$. Let $\zeta$ be a primitive $m$-th root of 1. Show that

$$\frac{\zeta^k - 1}{\zeta - 1}$$

is a unit in $\mathcal{O}(\mathbb{Q}(\zeta))$.

**19.** Let $\alpha \in \mathbb{C}$ be a root of $x^3 - x - 1$. (We may assume without proof that $\mathcal{O}(\mathbb{Q}(\alpha)) = \mathbb{Z}[\alpha]$.) Prove that

$$(23) = (23, \alpha - 10)^2(23, \alpha - 3)$$

is the prime ideal factorisation of the principal ideal $(23) \lhd \mathcal{O}$.

**20.** Let $F$ be a field and $R = F[x]$ a PID. Thus an $R$-module is automatically an $F$-vector space where the action of $x$ is a linear transformation. Let $V$ be an $R$-module that is finite dimensional over $F$. Then it is also finitely generated so we can apply the fundamental theorem and conclude that $V \cong V_i$, where each $V_i \cong R/(p_i(x)^{a_i})$, $p_i(x) \in R$ irreducible. Show that if $F$ is algebraically closed then the action of $x$ on is that of a Jordan block. (Can you describe the action of $x$ on $V_i$ if $p_i(x)$ is not irreducible?)