EXERCISE SHEET 1: ALGEBRAIC NUMBER THEORY SUMMER SCHOOL AT AMSS 2019

Exercise 1. The aim of the exercise is to prove that if $\alpha \in \mathbb{C}$ is an algebraic integer such that $|\sigma(\alpha)| = 1$ for all $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$, then α must be a root of unity.

(1) Show that if $f(X) \in \mathbb{C}[X]$ be a monic polynomial such that all its roots have complex absolute value 1, then the coefficient of X^r in $f(X)$ is bounded by $\binom{n}{r}$.
(2) Show that given an integer $n \geq 1$, there exist only finitely many algebraic integers α of degree n such that $|\sigma(\alpha)| = 1$ for all $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$.
(3) Show that an α as in (2) is a root of unity.

Exercise 2. Let $f(x) = x^3 + ax + b$ be an irreducible polynomial over $\mathbb{Q}$, and $\alpha \in \mathbb{C}$ be a root of $f(x)$. Set $K = \mathbb{Q}[\alpha]$, and $\mathcal{O}_K$ to be its ring of integers.

(1) Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$.
(2) Find an irreducible polynomial for $2a\alpha + 3b$ over $\mathbb{Q}$.
(3) Show that $\mathrm{Disc}_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -(4a^3 + 27b^2)$.
(4) Prove that $f(x)$ is irreducible when $a = b = -1$, and find an integral basis of K.

Exercise 3. Consider the number field $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$, and let $\mathcal{O}_K$ be its ring of integers. The aim of this exercise is to show that there exists no algebraic integer α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(1) Consider the elements:

$$\begin{aligned}
\alpha_1 &= (1+\sqrt{7})(1+\sqrt{10}),\\
\alpha_2 &= (1+\sqrt{7})(1-\sqrt{10}),\\
\alpha_3 &= (1-\sqrt{7})(1+\sqrt{10}),\\
\alpha_4 &= (1-\sqrt{7})(1-\sqrt{10}).
\end{aligned}$$

Show that for any $i \neq j$, the product $\alpha_i\alpha_j$ is divisible by 3 in $\mathcal{O}_K$.

(2) Let $i \in \{1, 2, 3, 4\}$ and $n \geq 0$ be an integer. Show that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n \equiv (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \mod 3.$$

Deduce that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i) \equiv 1 \mod 3$ and hence 3 does not divide α_i in $\mathcal{O}_K$.

(3) Let α be an algebraic integer. Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α. For all polynomial $g \in \mathbb{Z}[X]$, we denote by $\bar{g} \in \mathbb{F}_3[X]$ its reduction modulo 3. Show that $g(\alpha)$ is divisible by 3 in $\mathcal{O}_K$ if and only if $\bar{g}$ is divisible by $\bar{f}$ in $\mathbb{F}_3[X]$.
(4) For $1 \leq i \leq 4$, let $g_i(X) \in \mathbb{Z}[X]$ be such that $\alpha_i = g_i(\alpha)$. Show that there exists an irreducible factor of $\bar{f}$ that divides $\bar{g}_j$ for any $j \neq i$ but does not divide $\bar{g}_i$.
(5) Consider the number of irreducible factors of $\bar{f}$ and deduce a contradiction.

EXERCISE SHEET 2: ALGEBRAIC NUMBER THEORY
SUMMER SCHOOL AT AMSS 2019

Exercise 1. Find an integral basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Exercise 2. Let ζ_N be a primitive N-th root of unity. Put $\theta = \zeta_N + \zeta_N^{-1}$.

(1) Show that $\mathbb{Q}(\theta)$ is the fixed field of $\mathbb{Q}(\zeta_N)$ under the automorphism defined by the complex conjugation.
(2) Put $n = \phi(N)/2$. Show that $\{1, \zeta_N, \theta, \theta\zeta_N, \theta^2, \theta^2\zeta_N, \cdots, \theta^{n-1}, \theta^{n-1}\zeta_N\}$ is an integral basis for $\mathbb{Q}(\zeta_N)$.
(3) Show that the ring of integers of $\mathbb{Q}(\theta)$ is $\mathbb{Z}[\theta]$.
(4) Suppose that $N = p$ is an odd prime number. Prove that the discriminant of $\mathbb{Q}(\theta)$ is $\Delta_{\mathbb{Q}(\theta)} = p^{\frac{p-3}{2}}$.

Exercise 3. Let A be a local domain with unique maximal ideal $\mathfrak{m} \subset A$ such that each non-zero ideal $I \subseteq A$ admits a unique factorization $I = \prod_i \mathfrak{p}_i^{e_i}$ into products of prime ideals $\mathfrak{p}_i$.

(1) Show that there exists $x \in \mathfrak{m} \backslash \mathfrak{m}^2$.
(2) Let $x \in \mathfrak{m} \backslash \mathfrak{m}^2$ and $y \in \mathfrak{m}$. Prove that $(x, y) \subseteq A$ is prime ideal.
    Hint: Write $(x, y) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ as a product of prime ideals and use $x \notin \mathfrak{m}^2$
(3) Prove $(x) = \mathfrak{m}$.
    Hint: For $y \in \mathfrak{m}$, show $y \in (x, y^2)$.
(4) Conclude that every element $y \in A\backslash\{0\}$ admits a unique expression $y = ux^e$ with $e \geqslant 0$ and $u \in A^\times$ a unit and that A is a discrete valuation ring.

Exercise 4 (Chinese Remainder Theorem)**.** Let A be a commutative ring, $I, J \subseteq A$ be ideals such that $1 \in I + J$. Consider the natural map $\phi : A/I \cap J \to A/I \oplus A/J$ sending x to $(x \mod I, x \mod J)$.

(1) Prove that, given any $x \in A$, there exists $y \in I$ such that $y \equiv x \mod J$ (Hint: write $1 = a + b$ for some $a \in I$ and $b \in J$).
(2) Use (1) to prove ϕ is an isomorphism.
(3) Suppose that A is a Dedekind domain. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be primes of A such that $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$, and $e_1, \cdots, e_r \geqslant 1$ be integers. Prove that

$$A/\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} = \bigoplus_{i=1}^{r} A/\mathfrak{p}_i^{e_i}.$$

EXERCISE SHEET 3: ALGEBRAIC NUMBER THEORY SUMMER SCHOOL AT AMSS 2019

Exercise 1. Let $A = \mathbb{Z}[\sqrt{-1}]$.

(1) Find all the ideals $I \subseteq A$ with norm 65 (Hint: note that A is PID. Solve first the problem with 65 replaced by 5 and 13.).
(2) Are there infinitely many *fractional ideals* I of A with norm 1?

Exercise 2. Let $K = \mathbb{Q}(\alpha)$ with $\alpha^3 = \alpha + 1$.

(1) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
(2) Find the explicit decomposition of primes $p = 3, 5, 23$ in $\mathcal{O}_K$.
(3) Prove that $\sqrt{\alpha}, \sqrt[3]{\alpha} \notin K$. (Hint: try to find prime p such that there exists a surjective map $\mathcal{O}_K \twoheadrightarrow \mathbb{F}_p$ such that the image of α can not has square or cubic root.)

Exercise 3. Let $K = \mathbb{Q}(\alpha)$ with $\alpha^5 = 2$.

(1) Determine all the primes p that are ramified in K.
(2) Prove that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
(3) Prove that if p is a prime unramified in K and $5 \nmid (p^2 - 1)$, then p decomposes in $\mathcal{O}_K$ as $(p) = \mathfrak{p}\mathfrak{p}'$ with $f(\mathfrak{p}|p) = 1$ and $f(\mathfrak{p}'|p) = 4$.

Exercise 4. Let $K/\mathbb{Q}$ be a finite extension and K^{Gal} be the Galois closure of K. Prove that if a prime p is unramified in K, it is also unramified in K^{Gal}.