HEIGHTS PROBLEM SET 3

Below you will find some problems to work on for Week 3! There are three categories: beginner, intermediate and advanced.

Beginner problems

Question 1. Prove that for every algebraic number α, there is a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

Question 2.

(1) If α is an algebraic integer with minimal polynomial f of degree n, prove that the discriminant of the power basis generated by α is precisely the discriminant of the polynomial f, and we have $\Delta(\alpha) := \Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$. In particular, if $f(x) = x^2 + ax + b$, then the corresponding discriminant is $b^2 - 4a$ and if $f(x) = x^3 + ax + b$, then the corresponding discriminant is $-4a^3 - 27b^2$.

(2) Let p be a prime and let φ_p be the p-th cyclotomic polynomial. That is

$$\varphi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Show that the discriminant of the power basis generated by a primitive p-th root of unity ζ_p is $(-1)^{\binom{p-1}{2}} p^{p-2}$. (Hint: Use the equality $\varphi_p(x)(x-1) = x^p - 1$ and the product rule of differentiation to simplify $\varphi_p'(\zeta_p)$.)

Question 3. Verify that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are four mutually non-associate irreducible elements in the ring $\mathbb{Z}[\sqrt{-5}]$ that are not prime.

Question 4. Let $K/\mathbb{Q}$ be a degree n number field.

(1) Prove that if I is a nonzero ideal of $\mathcal{O}_K$, then there is a nonzero integer m in $I \cap \mathbb{Z}$.

(2) Show that every nonzero ideal I is a sublattice of $\mathcal{O}_K$ of maximal rank, i.e. I has finite index in $\mathcal{O}_K$, and is isomorphic to $\mathbb{Z}^n$ as an abelian group.

Question 5. Let $K = \mathbb{Q}(\sqrt{-23})$.

(a) Find $\mathcal{O}_K$.

(b) Prove that the norm map $N : K \to \mathbb{Q}$ taking $\alpha \to \alpha\sigma(\alpha)$, where σ is complex conjugation, takes values in $\mathbb{Z}$ when restricted to $\mathcal{O}_K$.

(c) Show that 2 is irreducible in $\mathcal{O}_K$ but not prime. Conclude that $\mathcal{O}_K$ is not a UFD.

Question 6. Verify that $\sqrt{2} + 1$ is a unit in the ring $\mathbb{Z}[\sqrt{2}]$. Use the Minkowski embedding to show that $\sqrt{2} + 1$ has infinite order in the group of units of $\mathbb{Z}[\sqrt{2}]$.

Intermediate problems

Question 7. Consider the elliptic curve $E : y^2 = x^3 - 2$. In this exercise, we will find all integer points on this curve. Fix any $x, y \in \mathbb{Z}$ satisfying $y^2 = x^3 - 2$.

(1) Show that y is odd.

(2) Note that if we work in the ring $\mathbb{Z}[\sqrt{-2}]$, then we can write

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

Take for granted the fact that $\mathbb{Z}[\sqrt{-2}]$ is a UFD (see Question 14), and show that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime.

(3) Show that there must exist some unit $u \in \mathbb{Z}[\sqrt{-2}]^\times$ and some $\alpha \in \mathbb{Z}[\sqrt{-2}]$ so that

$$y + \sqrt{-2} = u\alpha^3.$$

(4) Show that we can always take $u = 1$ above (Hint: if $\alpha \in \mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$, its complex norm $|\alpha|$ is an integer. Use this to compute $\mathbb{Z}[\sqrt{-2}]^\times$.)

(5) At this point, $y + \sqrt{-2}$ must be a cube in $\mathbb{Z}[\sqrt{-2}]$. Directly compute all (finitely many) possible values of y, and then use this to find all integral points of E (See footnote for the end result[1]).

Question 8. Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{-2})$. Enlarge the finite index subgroup of $\mathcal{O}_K$ spanned by $1, \sqrt{7}, \sqrt{-2}, \sqrt{-14}$ to a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

Question 9. Let K be a number field of degree n and $\beta_1, \ldots, \beta_n$ be $\mathbb{Q}$-linearly independent algebraic integers in K. Show that the lattice Λ spanned by the images of the β_i has rank n in $\mathbb{R}^n$ and that the fundamental domain of Λ has volume $2^{-s}\sqrt{|\Delta(\beta_1, \beta_2, \ldots, \beta_n)|}$, where s is the number of pairs of complex embeddings of K.

Problems 10 and 11 involve working with Galois extensions. Recall that a Galois extension K/F is a field extension $F \subseteq K$ such that

(1) the extension is *finite*: the dimension of K as a vector space over F, denoted by $[K : F]$, is finite.
(2) the extension is *algebraic*: for every $\alpha \in K$, there is a nonzero polynomial with coefficients in F such that α is a root of this polynomial;
(3) the extension is *normal*: Every polynomial in $F[x]$ that has a root in K has all roots in K;
(4) the extension is *separable*: For every $\alpha \in K$, its minimal polynomial is separable (does not have repeated roots).

Equivalently, an extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. If K/F is Galois, then we define $\mathrm{Gal}(K/F)$, the Galois group of K/F, to be the group $\mathrm{Aut}(K/F)$. This is, $\mathrm{Gal}(K/F)$ is the group of field automorphisms of K that fix F.

Question 10.
Consider the natural action of S_n on $\mathbb{Z}[x_1, x_2, \ldots, x_n]$, namely the permutation action on the indices of the variables. Let $r_D = \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ and let $D = r_D^2$.

(1) Let $\sigma \in S_n$. Show that $\sigma(D) = D$ for all $\sigma \in S_n$ and that $\sigma(r_D) = r_D$ if and only if $\sigma \in A_n$.
(2) Now let p be an irreducible cubic polynomial in $\mathbb{Q}[x]$. Let E be the splitting field of p over $\mathbb{Q}$, let $\alpha_1, \alpha_2, \alpha_3$ be the roots of p in E and let $G := \mathrm{Gal}(E/\mathbb{Q})$. Show that G is either A_3 or S_3.
(3) Let G be as above. show that $G = A_3$ if and only if $r_D(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Q}$. (In other words, the discriminant of the polynomial p is a square in $\mathbb{Q}$ if and only if the splitting field of p is a cubic Galois A_3 extension.) [2]

Question 11.

(1) Let $p(x) = x^3 - 21x - 7$. Show that p is an irreducible polynomial in $\mathbb{Z}[x]$. (Caution: Remember that there is one extra step in going from being irreducible in $\mathbb{Q}[x]$ to being irreducible in $\mathbb{Z}[x]$). Graph the polynomial p and show that all its roots are real.
(2) Compute the discriminant of the polynomial p and show that the splitting field of p is a cubic Galois A_3 extension of $\mathbb{Q}$. [3] (Hint: use Question 10).
(3) Show that if the splitting field of an irreducible cubic polynomial over $\mathbb{Q}$ is an A_3 extension, then all the roots of the cubic in $\mathbb{C}$ are real. (Remark: The converse is not necessarily true, but an explicit example does not come to mind. Let me know if you find one!)

[1] You should find that the only integer solutions to $y^2 = x^3 - 2$ are $(x, y) = (3, \pm 5)$

[2] See sections 14.6 and 14.7 of Dummit and Foote for explicit solutions to cubic and quartic polynomials over $\mathbb{Q}$ by radicals. The explicit forms of the solutions can be used to give an alternate proof for the problem above.

[3] This is one of the extensions that shows up when you try to write down a primitive 7-th root of unity explicitly in terms of radicals.

Advanced problems

Question 12. Consider the affine elliptic curve with equation $y^2 - x^3 + x \in \mathbb{C}[x, y]$ and its associated affine coordinate ring $S := \mathbb{C}[x, y]/(y^2 - x^3 + x)$.

(1) Let a be a complex number. Prove that if $a \notin \{-1, 0, 1\}$, then $S/(x-a)S$ has exactly two prime ideals, whose lifts $\mathfrak{p}_1, \mathfrak{p}_2$ to S satisfy $(x - a)S = \mathfrak{p}_1\mathfrak{p}_2$ (the "completely split" case), and that if $a \in \{-1, 0, 1\}$, then $S/(x-a)S$ has a unique prime ideal $\mathfrak{p}$ and $(x-a)S = \mathfrak{p}^2$ (the "ramified" case).

(2) Show that every nonzero prime ideal of S is of the form $(x - a, y - b)$ for some complex numbers a and b. (Hint: Show that the intersection of a nonzero prime ideal of S with $\mathbb{C}[x]$ is a *nonzero prime* ideal of $\mathbb{C}[x]$, and hence of the form $(x - a)$ for some complex number a.)

Question 13. Let p be a prime number, and let $K = \mathbb{Q}(\zeta_p)$, where $\zeta = \zeta_p$ is a primitive pth root of unity. In this problem, we want to compute the ring of integers $\mathscr{O}_K$. First, recall from Question 2 that $\mathbb{Z}[\zeta_p]$ has discriminant $\pm$(power of p). Recall also from lecture that

$$\Delta(\zeta_p) = [\mathscr{O}_K : \mathbb{Z}[\zeta_p]]^2\Delta_K.$$

(1) Deduce that the index of $\mathbb{Z}[\zeta_p]$ in $\mathscr{O}_K$ is a power of p. Suppose that $(p\mathscr{O}_K \cap \mathbb{Z}[\zeta_p]) = p\mathbb{Z}[\zeta_p]$. Use this to show that $\mathscr{O}_K = \mathbb{Z}[\zeta_p]$.

(2) Note that the minimal polynomial of $\zeta - 1$ is

$$f(x) = \varphi_p(x + 1) = \frac{(x + 1)^p - 1}{x}.$$

Show that $f(x)$ is p-Eisenstein[4]. Use this to show that $(\zeta - 1)^{p-1} \mid p$ in $\mathbb{Z}[\zeta]$.

(3) Show that $(p\mathscr{O}_K \cap \mathbb{Z}[\zeta_p]) = p\mathbb{Z}[\zeta_p]$ (Hint: $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$, so any $x \in p\mathscr{O}_K \cap \mathbb{Z}[\zeta_p]$ can be written as

$$x = c_0 + c_1(\zeta - 1) + \cdots + c_d(\zeta - 1)^d$$

where $d = [K : \mathbb{Q}] - 1 = p - 2$ and $c_i \in \mathbb{Z}$. Inductively show that $p \mid c_i$).

Question 14. Show that the ring $\mathbb{Z}[\sqrt{-2}]$ is a UFD (Hint: it suffices to show that it is a Euclidean domain).

References

[Wal00] Michel Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 326, Springer-Verlag, Berlin, 2000. Transcendence properties of the exponential function in several variables. MR1756786 ↑

[4] i.e. $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ where $p \nmid a_0$, $p^2 \nmid a_n$, but $p \mid a_i$ for all $i > 0$ (including $i = n$)