Exercises for Ila Varma's problem session
BRIDGES Conference 2024
University of Utah

July 10, 2024

1 Quadratic fields

1.1 Algebraic

Exercise 1. The *ring of integers* of a number field K is the subset of elements of K which are roots of monic integer-coefficient polynomials.

a) Can you describe the ring of integers of $\mathbb{Q}(\sqrt{d})$?

   Hint: The ring of integers contains $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Does it contain any other elements of $\mathbb{Q}(\sqrt{d})$?

b) Describe all field automorphisms of $\mathbb{Q}(\sqrt{d})$ that fix $\mathbb{Q}$ pointwise.

   Choose an embedding $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ and compose with the field automorphisms you described above to get the full set of injective homomorphisms $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$.

c) The *discriminant* of a quadratic field is defined in terms of a basis of the ring of integers $\mathcal{O}_K$ (as a module over $\mathbb{Z}$) and injective ring homomorphisms $K \to \mathbb{C}$. Namely, if σ_1, σ_2 denote the injective ring homomorphisms and $\langle \alpha_1, \alpha_2 \rangle$ denote the basis elements over $\mathbb{Z}$ for $\mathcal{O}_K$, then

$$\operatorname{disc}(K) := \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) \end{pmatrix}^2$$

   Give a formula for the discriminant of a quadratic field $\mathbb{Q}(\sqrt{d})$.

1.2 Analytic

Exercise 2. Prove that

$$\lim_{x \to \infty} \frac{\#\{\mathbb{Q}(\sqrt{d}) : |\operatorname{disc}(\mathbb{Q}(\sqrt{d}))| \leq x\}}{x} = \frac{1}{\zeta(2)}$$

where $\zeta(2) = \sum_{n \geq 1} \frac{1}{n^2}$.

Exercise 3. Prove that $\zeta(2) = \frac{6}{\pi^2}$.

2 Cubic fields

Exercise 4 (Difficult)**.** Is there a criterion for when α, a root of a cubic polynomial $f(x)$, and β, a root of another cubic polynomial $g(x)$, generate the same cubic field, i.e. $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$?

Exercise 5. A rank 3 $\mathbb{Z}$-module's basis can be written as $\langle 1, \omega, \theta \rangle$. If that rank 3 $\mathbb{Z}$-module happens to be a ring, then that implies that

$$\begin{aligned} \omega^2 &= a + b\omega + c\theta & a, b, c &\in \mathbb{Z} \\ \omega\theta &= d + e\omega + f\theta & d, e, f &\in \mathbb{Z} \\ \theta^2 &= g + h\omega + i\theta & g, h, i &\in \mathbb{Z} \end{aligned}$$

a) Can you find a change-of-basis matrix γ to apply to $\langle 1, \omega, \theta \rangle$ so that the new basis $\langle 1, \omega', \theta' \rangle$ satisfies $\omega'\theta' \in \mathbb{Z}$?

b) Assume $\langle 1, \omega, \theta \rangle$ satisfies $\omega\theta \in \mathbb{Z}$. Can you find relations between $a, b, c, d, e, f, g, h, i$?

c) Assume $\langle 1, \omega, \theta \rangle$ satisfies $\omega\theta \in \mathbb{Z}$. Can you find all other bases for the same rank 3 ring as generated by $\langle 1, \omega, \theta \rangle$ that have 1 as the first basis element and the product of the other two is in $\mathbb{Z}$?