Algebraic number theory — Exercise sheet 5 (optional)

https://www.maths.tcd.ie/~mascotn/teaching/2022/MAU34109/index.html

Version: November 22, 2022

Exercise 5.1: Units in a real quadratic field

Let $K = \mathbb{Q}(\sqrt{42})$, viewed as a subfield of $\mathbb{R}$.

1. Find a fundamental unit ε in K such that $\varepsilon > 1$.

2. Prove that the equation $x^2 - 42y^2 = -1$ has no solutions in integers.

   Hint: Write down generators for $\mathbb{Z}_K^\times$. What are their norms?

   We now wish to determine the class group $\mathrm{Cl}(K)$ of K.

3. First of all, prove that it is generated by the image of the prime $\mathfrak{p}_2$ above 2, and that this image has order at most 2 in $\mathrm{Cl}(K)$.

4. We want to prove that $\mathfrak{p}_2$ is not principal. Suppose by contradiction that it is, and let $\gamma = x + y\sqrt{42}$ be a generator. Explain why we may assume that $\frac{1}{\sqrt{\varepsilon}} \leq \gamma \leq \sqrt{\varepsilon}$, and deduce that $|y| < 2$.

5. Prove that $\mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercise 5.2: Arbitrary unit groups

1. Prove that there is no number field K such that the unit group $\mathbb{Z}_K^\times$ is isomorphic to $\mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}^{10}$.

2. Find a number field K such that $\mathbb{Z}_K \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$.

Exercise 5.3: A lower bound on the regulator

Let K be a number field of degree 3 such that $\operatorname{disc} K < 0$.

1. Prove that the signature of K is $(1, 1)$.

2. From now on, we let σ be the unique real embedding of K. Prove that there exists $\varepsilon \in K$ such that $\mathbb{Z}_K^\times = \{\pm\varepsilon^n,\ n \in \mathbb{Z}\}$ and that $\sigma(\varepsilon) > 1$, and that such an ε is unique.

3. Prove that ε is a primitive element for K, and deduce that the minimal polynomial of ε factors over $\mathbb{R}$ as $(x - \sigma(\varepsilon))(x - u^{-1}e^{i\theta})(x - u^{-1}e^{-i\theta})$ for some $\theta \in \mathbb{R}$, where $u = \sqrt{\sigma(\varepsilon)}$.

4. Using without proof the fact that

$$\left(\frac{u^3 + u^{-3}}{2} - \cos\theta\right)^2 \sin^2\theta < \frac{u^6}{4} + \frac{3}{2}$$

   for all $\theta \in \mathbb{R}$ (you are **NOT** required to prove this), prove that

$$\sigma(\varepsilon) > \sqrt[3]{\frac{|\operatorname{disc} K|}{4} - 6}.$$

   Hint: Prove that

$$\operatorname{disc} \mathbb{Z}[\varepsilon] = -16\left(\frac{u^3 + u^{-3}}{2} - \cos\theta\right)^2 \sin^2\theta.$$

5. As an application, we want to find a fundamental unit in $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^3 + 4x + 2$. We admit without proof that the only real root of $f(x)$ is approximately -0.473, and still denote by σ the corresponding embedding of K into $\mathbb{R}$.

   (a) By taking a look at the decomposition of $2\mathbb{Z}_K$, find a unit $u \in \mathbb{Z}_K^\times$ such that $\sigma(u) > 1$.

   (b) Prove that u is either a fundamental unit or the square of a fundamental unit.

   (c) By reducing u mod one of the primes above 3, prove that u is actually a fundamental unit.

   (d) What is the regulator of K?

Exercise 5.4: Units in a real cubic field

For this exercise, you will need a calculator so as to compute complex embeddings explicitly. Do not worry about accuracy issues.

Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - 12x + 6$. You will need to know the following:

- The roots of f are approximately -3.69, 0.511, and 3.18.
- f Assumes the following values:

x	-5	-4	-3	-2	-1	0	1	2	3	4	5
$f(x)$	-59	-10	15	22	17	6	-5	-10	-3	22	71

- The regulator of K is[1] approximately 21.

1. Prove that f is irreducible over $\mathbb{Q}$, and that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.
2. Determine W_K and the rank of $\mathbb{Z}_K^\times$.
3. Determine explicitly the decomposition of 2, 3, and 5 in K.
4. Use the formula $N_{\mathbb{Q}}^K(\alpha + n) = -f(-n)$ to prove that $\alpha - 3$ generates the prime above 3. Explain how to use this to discover that $u = (\alpha - 3)^3/3$ is a unit in K.
5. Factor the ideals $(\alpha - 1)$ and $(\alpha + 4)$ into primes. Use this to find a generator γ for the prime above 2, and deduce that $v = \gamma^3/2$ is also a unit in K.

   I recommend you ***NOT*** *to try to express γ and v as polynomials in α.*
6. Compute approximately the regulator of $\{u, v\}$.
7. Let U be the subgroup of $\mathbb{Z}_K^\times$ generated by W_K, u, and v. Is U equal to $\mathbb{Z}_K^\times$? What is the (possibly infinite) index of U in $\mathbb{Z}_K^\times$?
8. Compute the factorisation of the ideal (α) into primes, and use it to find a third unit $w \in \mathbb{Z}_K^\times$.
9. Prove that $\{u, w\}$ is a system of fundamental units for K.
10. Use the logarithmic embedding to conjecture a simple expression for v in terms of u and w (you do not have to prove that your conjecture is correct). Is your guess compatible with question 7?

[1] I determined this using a computer and methods beyond the scope of this class.