Solutions to Sheet 12

Exercise 1

Let I be an ideal of a number field K. Show that htere is a finite field extension L of K such that $I\mathcal{O}_L$ is a principal ideal of $\mathcal{O}_L$.

Solution. By finiteness of $\mathrm{Cl}(K)$ there is some integer m such that $[I]^m = [I^m] = [(1)] \in \mathrm{Cl}(K)$, i.e., $I^m = (\alpha)$ is a principal ideal. We put $L = K(\alpha^{1/m})$. Now $\alpha^{1/m} \in \mathcal{O}_L$, and we have

$$(I\mathcal{O}_L)^m = I^m\mathcal{O}_L = \alpha\mathcal{O}_L = (\alpha^{1/m})^m\mathcal{O}_L.$$

After decomposing $I\mathcal{O}_L$ and $\alpha^{1/m}\mathcal{O}_L$ into prime factors, we see that this equation implies $I\mathcal{O}_L = \alpha^{1/m}\mathcal{O}_L$.

Exercise 2

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and set

$$\Gamma = \{(1+\sqrt{2})^i(2+\sqrt{3})^j(\sqrt{2}+\sqrt{3})^k \mid i,j,k \in \mathbb{Z}\}.$$

Show that Γ is a subgroup of $\mathcal{O}_K^\times$ and that $[\mathcal{O}_K^\times : \Gamma] < \infty$.

Solution. Write u, v, w for the respective factors, so that $\Gamma = u^{\mathbb{Z}}v^{\mathbb{Z}}w^{\mathbb{Z}}$. Note that $\mathrm{N}_{K/\mathbb{Q}}(u) = \mathrm{N}_{K/\mathbb{Q}}(v) = 1$ and $\mathrm{N}_{K/\mathbb{Q}}(w) = -1$, so that indeed, u, v, w are units and Γ is a subgroup of $\mathcal{O}_K^\times$. One quickly verifies that K is totally real. Indeed, it is Galois and there is a embedding $K \hookrightarrow \mathbb{R}$ (now all other embeddings are obtained by shifting with elements in the Galois group). Hence, by Dirichlet's unit theorem,

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1} = \pm 1 \times \mathbb{Z}^3.$$

On the other hand, Γ is free of rank 3. Indeed, $u \in \mathbb{Q}(\sqrt{2})^\times$, $v \in \mathbb{Q}(\sqrt{3})^\times$ and $w \in \mathbb{Q}(\sqrt{2},\sqrt{3})^\times \setminus (\mathbb{Q}(\sqrt{2})^\times \cup \mathbb{Q}(\sqrt{3})^\times) \cup \{1\}$. These multiplicative subsets of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ only have trivial intersection.

Let $\mathcal{O}_{K,>0}^\times \cong \mathbb{Z}^3$ be the (free) group of positive units (here we implicitly fix a inclusion $K \hookrightarrow \mathbb{R}$). Now Γ is a free subgroup of full rank this group, and in particular, its has finite index. The inclusion $\mathcal{O}_{K,>0}^\times \hookrightarrow \mathcal{O}_K^\times$ also has finite index, hence $\Gamma \hookrightarrow \mathcal{O}_K^\times$ has finite index.

Exercise 3

Let K be a totally real number field, i.e., one that has **only** real embeddings. Let

$$T \subset \mathrm{Hom}(K, \mathbb{R}) = \{\tau : K \to \mathbb{R} \mid \tau \text{ is a field homomorphism}\}$$

be a proper non-mepty subset. Show that there exists $u \in \mathcal{O}_K^\times$ such that $0 < \tau(u) < 1$ for $\tau \in T$ and $\tau(u) > 1$ for $\tau \in \mathrm{Hom}(K,\mathbb{R}) \setminus T$.

Solution. Let $\sigma_1, \ldots, \sigma_r : K \to \mathbb{R}$ be the real embeddings of K (in our case $r = n = [K : \mathbb{Q}]$). From the proof of Dirichlet's unit theorem, we know that the map

$$\mathcal{L} : \mathcal{O}_K^\times \to \mathbb{R}^r, \quad u \mapsto (\log|\sigma_1(u)|, \ldots, \log|\sigma_r(u)|)$$

is a group homomorphism from $\mathcal{O}_K$ to $\mathbb{R}^{r-1}$. It's image lies in the sub vector space V given by

$$V = \left\{ (x_1, \ldots, x_r)^t \in \mathbb{R}^r \mid \sum_{i=1}^{r} x_i = 0 \right\},$$

and its kernel is given by $\mu(K)$, the group of roots of unity in K (in our case this is $\cong \{\pm 1\}$). Also, the image $\mathcal{L}(\mathcal{O}_K^\times)$ has full rank in V, i.e., $\mathcal{L}(\mathcal{O}_K^\times) \otimes_{\mathbb{Z}} \mathbb{R} \cong V$ (it is a lattice in V).

Without loss of generality we can assume that $T = \{\sigma_1, \ldots, \sigma_q\}$ for some $1 \leq q < r$. Let $Q \subset \mathbb{R}^r$ be the quadrant given by

$$Q = \{(x_1, \ldots, x_r)^t \in \mathbb{R}^r \mid x_i < 0 \text{ for } i = 1, \ldots, q \text{ and } x_i > 0 \text{ for } i = q+1, \ldots, r\}.$$

The intersection $Q \cap V$ is non-empty by construction, and one readily verifies that there is a point $x \in Q \cap \mathcal{L}(\mathcal{O}_K^\times)$. Now choose some preimage $u \in \mathcal{O}_K^\times$ of x. As u satisfies $|\sigma_i(u)| < 1$ for $1 \leq i \leq q$ and $|\sigma_i(u)| > 1$ for $q < i \leq r$, the element u^2 satisfies all constraints.

Exercise 4

Let K be a number field, let I be a non-zero ideal of $\mathcal{O}_K$ and let $C \in \mathrm{Cl}(K)$. Use theorem 5.3 to show that there exists a non-zero ideal J of $\mathcal{O}_K$ such that $I + J = \mathcal{O}_K$ and $C = [J]$.

Solution. Theorem 5.3 counts the number of objects in an ideal class up to some given norm t. For $C \in \mathrm{Cl}(K)$, let $i(K, C, t)$ be the set of ideal in the given ideal class C with norm $\leq t$ (just as in the statement). Then theorem 5.3 reads

$$i(K, C, t) = \kappa t + O(t^{1-1/d}) = \kappa t + o(t).$$

Here we used *big-O-notation*, the equation above means essentially is that $i(K, C, t)$ is of size κt up to an error that is bounded by some multiple of $t^{1-1/d}$. Let's solve the exercise. We will show that the set of ideals

$$\{J \subset \mathcal{O}_K \mid J \in C \& J + I = \mathcal{O}_K \& \mathrm{N}(J) \leq t\}$$

is non-epty for t sufficiently large. Note that two ideals are coprime if and only if they don't share a prime factor.

If we assume that $I = \mathfrak{p}$ is prime, we use that

$$\begin{aligned}
&\#\{J \mid \mathrm{N}(J) \leq t \wedge J + I = \mathcal{O}_K \wedge [J] = C\} \\
&\qquad = \#\{J \mid \mathrm{N}(J) \leq t \wedge [J] = C\} - \#\{J \mid \mathrm{N}(J) \leq t \wedge \mathfrak{p} \mid J \wedge [J] = C\} \\
&\qquad = \#\{J \mid \mathrm{N}\, J \leq t \wedge [J] = C\} - \#\{J \mid \mathrm{N}(J) \leq t/\mathrm{N}(\mathfrak{p}) \wedge [J] = C[p^{-1}]\} \\
&\qquad = i(K, C; t) - i(K, [p^{-1}]C; t/\mathrm{N}(\mathfrak{p}))\kappa t - \kappa \frac{t}{\mathrm{N}(\mathfrak{p})} + O(t^{1-1/d}) \\
&\qquad = \kappa \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right) t + O(t^{1-1/d}).
\end{aligned}$$

If $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, we use the same idea and inclusion-exclusion to find that

$$\begin{aligned}
&\#\{J \mid \mathrm{N}(J) \le t \wedge J + I = \mathcal{O}_K \wedge [J] = C\} \\
&\qquad = \sum_{k=0}^{n} \sum_{S \subset \{1,\dots,n\}, |S|=k} (-1)^k \# \left\{ J \mid \mathrm{N}(J) \le \frac{t}{\prod_{s \in S} \mathrm{N}(\mathfrak{p}_s)} \wedge [J] = \left[\prod_{s \in S} \mathfrak{p}_s^{-1} \right] C \right\} \\
&\qquad\qquad = \sum_{k=0}^{n} (-1)^k \sum_{S \subset \{1,\dots,n\},\ |S|=k} (-1)^k \kappa t \prod_{s \in S} \mathrm{N}(\mathfrak{p}_s)^{-1} + O(t^{1-1/d}) \\
&\qquad\qquad\qquad = \kappa t \prod_{\mathfrak{p} \mid I} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})} \right) + O(t^{1-1/d}).
\end{aligned}$$

If t is sufficiently large, this is positive. This result has a nice interpretation, the factor $\prod(1 - \frac{1}{\mathrm{N}(\mathfrak{p})})$ is (in some sense) the probability of a random ideal to be coprime to I. So the result is what we would expect.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: January 22, 2024