Algebraic Number Theory 88-798

Remarks on Question Sheet 2

(1) The third exercise on Question Sheet 2 is the following:

Let $C \subset \mathbb{R}^n$ be bounded, convex, and symmetric. Let $v_1, \ldots, v_n \in \mathbb{R}^n$ be linearly independent vectors, and let A be the $n \times n$ matrix whose columns are the vectors v_i. Suppose that $\mathrm{vol}(C) > 2^n |\det A|$. Prove that there exist $x_1, \ldots, x_n \in \mathbb{Z}$, not all zero, such that $x_1 a_1 + \cdots x_n a_n \in C$.

Hint: Consider the set $D = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 a_1 + \cdots x_n a_n \in C\} \in \mathbb{R}^n$. We need to show that D contains a lattice point; a sketch of a proof follows. Show first that D is bounded, convex, and symmetric, and that $\mathrm{vol}(D) > 2^n$.

Let $D' \subset D$ be the subset consisting of points $(x_1, \ldots, x_n)$ such that $(2x_1, \ldots, 2x_n) \in D$. Then $\mathrm{vol}(D') > 1$. Let $\chi : \mathbb{R}^n \to \mathbb{R}$ be the characteristic function of D':

$$\chi(x) = \begin{cases} 1 & : x \in D' \\ 0 & : x \notin D' \end{cases}.$$

Now define the function $\psi : \mathbb{R}^n \to \mathbb{R}$ by

$$\psi(x) = \sum_{y \in \mathbb{Z}^n} \chi(x + y).$$

If $y \in \mathbb{Z}^n$ is a lattice point, it is clear that $\psi(x) = \psi(x + y)$, so that ψ induces a function on $\mathbb{R}^n/\mathbb{Z}^n$. The function is $\psi : \mathbb{R}^n/\mathbb{Z}^n \to \mathbb{R}$ is integrable, and

$$\int_{\mathbb{R}^n/\mathbb{Z}^n} \psi(x) dx = \mathrm{vol}(D') > 1.$$

Since $\mathrm{vol}(\mathbb{R}^n/\mathbb{Z}^n) = 1$ and ψ takes integer values, there must be a point $x \in R^n$ such that $\psi(x) \geq 2$. Equivalently, there exist two points $P_1, P_2 \in D'$ such that $P_1 - P_2 \in \mathbb{Z}^n$. Therefore, $2P_1, 2P_2 \in D$. By symmetry and convexity of D, it follows that the lattice point $P_1 - P_2$ is contained in D.

(2) Recall that for an ideal $\mathfrak{a} \subset \mathcal{O}_K$ we defined $N(\mathfrak{a})$ to be the cardinality of the quotient ring $\mathcal{O}_K/\mathfrak{a}$. We claimed that $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ and left this as an exercise. Here are some hints about how to do it. By the decomposition into primes it suffices to prove that if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are prime ideals and $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$, then $N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{e_i}$.

First show by the Chinese Remainder Theorem that $N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{p}_i^{e_i})$. To apply the Chinese Remainder Theorem, you will need to prove that $\mathfrak{p}_1^{e_1} + \mathfrak{p}_2^{e_2} = \mathcal{O}_K$ for any distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ and any exponents e_1, e_2. To see that, first obtain an expression

$x_1 + x_2 = 1$ for $x_i \in \mathfrak{p}_i$, which clearly exists by maximality of $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then,

$$(x_1 + x_2)^{e_1+e_2} = \sum_{j=0}^{e_1+e_2} \binom{e_1 + e_2}{j} x_1^j x_2^{e_1+e_2-j} = 1,$$

and it follows that $1 \in \mathfrak{p}_1^{e_1} + \mathfrak{p}_2^{e_2}$.

It remains to show that $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$ for any prime ideal $\mathfrak{p}$. To prove that, it suffices to show that the index of $\mathfrak{p}^e$ in $\mathfrak{p}^{e-1}$ is equal to the index of $\mathfrak{p}$ in $\mathcal{O}_K$. Let $x \in \mathfrak{p}^{e-1}$ be such that $x \notin \mathfrak{p}^e$. Then we claim that the map $f(y + \mathfrak{p}) = xy + \mathfrak{p}^e$ is an isomorphism of abelian groups

$$f : \mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^{e-1}/\mathfrak{p}^e.$$

Everything except the surjectivity of f is obvious. Consider the ideal $I = x\mathcal{O}_K + \mathfrak{p}^e \subset \mathcal{O}_K$. Then, $\mathfrak{p}^e \subseteq I \subseteq \mathfrak{p}^{e-1}$, and it follows by uniqueness of the prime decomposition that either $I = \mathfrak{p}^e$ or $I = \mathfrak{p}^{e-1}$. But $I = \mathfrak{p}^e$ is impossible, since $x \notin \mathfrak{p}^e$. Therefore $I = \mathfrak{p}^{e-1}$, which implies that f is surjective.