Autumn Semester 2019

# Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

## Solutions to Exercise Sheet 8

**Exercise 8.1.** Use the Minkowski bound $M_K = \frac{n!}{n^n}(4/\pi)^{r_2}|\Delta_K|^{1/2}$ to compute class numbers $h_K$ of the following fields.

(a) $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$.

(b) $K = \mathbb{Q}(\sqrt{-D})$ for $D = 11$ and $D = 19$.

**Solution.**
(a) We have $n = 3$, $r_1 = r_2 = 1$ and recall that $|\Delta_K| = 23$, thus $M_K = \frac{8\sqrt{23}}{9\pi} = 1.356... < 2$. Therefore, every ideal class contains an integral ideal of norm 1, i.e. $\mathcal{O}_K$, and hence every ideal is principal, so that $h_K = 1$.

(b) We have $M_K = \frac{2\sqrt{11}}{\pi} = 2.111... < 3$ or $M_K = \frac{2\sqrt{19}}{\pi} = 2.774... < 3$. Therefore, in both cases every ideal class contains an integral ideal of norm $\leq 2$.

Let us show that (2) is a prime ideal in $\mathbb{Q}(\sqrt{-D})$ for all $D \equiv 3 \pmod 8$. This implies that in these cases there are no ideals of norm 2, and thus $h_K = 1$ for $D = 11, 19$.

Let $\alpha = \frac{\sqrt{-D}-1}{2}$, where $D = 8k - 5$, so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\alpha^2 + \alpha + (2k-1) = 0$. Then $\mathcal{O}_K/2\mathcal{O}_K = \{\overline{0}, \overline{1}, \overline{\alpha}, \overline{\alpha+1}\}$. Since $\alpha(\alpha+1) = 1 - 2k \equiv 1 \pmod 2$, we get that $\overline{\alpha}$ and $\overline{\alpha+1}$ are invertible in $\mathcal{O}_K/(2)$, and hence $\mathcal{O}_K/(2)$ is a field. This shows that (2) is a prime ideal.

**Exercise 8.2.** Let $p$ be a prime congruent to 1 modulo 4. Recall that $-1$ is a quadratic residue, so that there exists $r \in \mathbb{Z}$ such that $p|r^2+1$. Consider the lattice $\Lambda \subset \mathbb{Z}^2$ generated by $(0,p)$ and $(1,r)$.

(a) Show that $\Lambda$ contains a vector of length less than $\sqrt{2p}$;

(b) Use (a) to prove that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

**Solution.** (a) Since $\det\begin{pmatrix} 0 & p \\ 1 & r \end{pmatrix} = -p$ we have that $|\Lambda| = p$. Note that the volume of the ball $B_{\sqrt{2p}}(0) \subset \mathbb{R}^2$ is $2\pi p > 4p$. Therefore, by Minkowski's theorem there exists a non-zero vector in $B_{\sqrt{2p}}(0) \cap \Lambda$.

(b) By part (a) there exists a non-zero vector $(a,b) = (l, kp+rl)$ such that $a^2+b^2 < 2p$. Since $a^2 + b^2 = p(k^2p + 2klr) + l^2(1+r^2) \equiv 0 \pmod p$ and $0 < a^2 + b^2 < 2p$, the only possibility is $a^2 + b^2 = p$.

**Exercise 8.3.** In this exercise we prove Lagrange's four-square theorem. Recall that the volume of a ball of radius $R$ in $\mathbb{R}^{2k}$ is $\frac{\pi^k R^{2k}}{k!}$.

(a) Verify Euler's identity

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax-by-cz-dt)^2+(ay+bx+ct-dz)^2 + (az-bt+cx+dy)^2+(at+bz-cy+dx)^2 .$$

(b) Show that for any prime $p$ there exist integers $r, s$ such that $p | r^2+s^2+1$.

(c) Consider the lattice $\Lambda = \{(a,b,c,d) \in \mathbb{Z}^4 \mid a \equiv rc+sd \pmod p, b \equiv rd-sc \pmod p\}$, where $r$ and $s$ are as in part (b). Show that the covolume of $\Lambda$ is $|\Lambda| = p^2$ and that there exists a nonzero vector $(a,b,c,d) \in \Lambda$ such that $a^2+b^2+c^2+d^2 < 2p$;

(d) Using (a) and (c) show that any non-negative integer can be written as a sum of four perfect squares.

**Solution.** (a) This is a direct calculation.

(b) If $p=2$ then $p = 1^2+0^2+1$. Assume that $p>2$ is odd. Note that there are $\frac{p+1}{2}$ square residues modulo $p$: $S = \{0^2, 1^2, \ldots, (\frac{p-1}{2})^2\} \subseteq \mathbb{Z}/p\mathbb{Z}$.

Let $A = S$ and $B = \{-1-s \mid s \in S\}$ be two subsets of $\mathbb{Z}/p\mathbb{Z}$. Since $|A| = |B| = \frac{p+1}{2}$ we have that $|A|+|B| = p+1 > p$. Hence $A \cap B \neq \emptyset$ and there exists some element $x \in A \cap B$. By definition this means that $x \equiv r^2 \pmod p$ and $x \equiv -1-s^2 \pmod p$ for some $r, s \in \mathbb{Z}$. But then $r^2+s^2+1 \equiv x-x \equiv 0 \pmod p$ as claimed.

(c) The lattice $\Lambda$ is generated by $(p,0,0,0)$, $(0,p,0,0)$, $(r,-s,1,0)$, $(s,r,0,1)$ (this is so since 3rd and 4th coordinates can be chosen freely and then the first two are uniquely determined modulo $p$). The determinant is

$$\det \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ r & -s & 1 & 0 \\ s & r & 0 & 1 \end{pmatrix} = p^2 .$$

Since the volume of the ball $B_{\sqrt{2p}}(0) \subset \mathbb{R}^4$ is $2\pi^2 p^2 > 2^4 p^2$, by Minkowski's theorem we get that there exists a non-zero vector $(a,b,c,d) \in \Lambda$ such that $a^2+b^2+c^2+d^2 < 2p$.

(d) The vector from part (c) satisfies $0 < a^2+b^2+c^2+d^2 < 2p$. Moreover,

$$\begin{aligned} a^2+b^2+c^2+d^2 &\equiv (rc+sd)^2+(rd-sc)^2+c^2+d^2 \\ &\equiv (c^2+d^2)(r^2+s^2+1) \equiv 0 \pmod p. \end{aligned}$$

Since the only multiple of $p$ between 0 and $2p$ is $p$ itself, we get $a^2+b^2+c^2+d^2 = p$. Therefore, every prime can be written as a sum of four squares. By part (a) if $n$ and $m$ can be written as sums of four squares of integers, then so is their product. Thus by factoring into primes we conclude that any positive integer can be written as a sum of four squares.

**Exercise 8.4*.** Show that for any $d$ there exist only finitely many number fields $K \subset \mathbb{C}$ of discriminant $\Delta_K = d$.

(*Hint: construct a convex body $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of volume $2^{n-r_2}|d|^{1/2}$ such that all but one of coordinates are bounded in absolute value by $1/2$ on $B$. Show that for any non-zero $x \in \mathcal{O}_K$ that maps to $B$ its minimal polynomial is of degree $n$ with bounded coefficients.*)

**Solution.** We let $d$ be fixed and let $K$ be a number field with $\Delta_K = d$. Without loss of generality assume that $n \geq 2$. Since the norm of any ideal is $\geq 1$ we have $M_K \geq 1$ and thus for all sufficiently large $n$ we have

$$|d|^{1/2} \geq \frac{n^n}{n!}(\pi/4)^{r_2} \geq \frac{(n\sqrt{\pi}/2)^n}{n!} \geq \frac{(n\sqrt{\pi}/2)^n}{n^2(n/e)^n} \geq \frac{2^n}{n^2},$$

where we have used $r_2 \leq n/2$ and $n! \leq n^2(n/e)^n$ that follows from Stirling's formula for sufficiently large $n$ (in fact the last inequality is true for all $n \geq 2$). Since $2^n/n^2 \to \infty$ as $n \to \infty$ and $d$ is fixed, the degree $n$ must be bounded, leaving only finitely many possibilities for $n$. Therefore, since $n = r_1 + 2r_2$, it is enough to show finiteness of the set of number fields of discriminant $d$ for fixed $r_1$ and $r_2$.

Let $i\colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the standard embedding. Define $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by requiring that $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in B$ if and only if

$$|y_1| \leq 2^n(2/\pi)^{r_2}|d|^{1/2}, \quad |y_j| \leq 1/2,\ j \geq 2, \quad |z_j| \leq 1/2,\ j \geq 1$$

if $r_1 > 0$ and

$$|\mathrm{Im}(z_1)| \leq 2^{n-1}(2/\pi)^{r_2-1}|d|^{1/2}, \quad |\mathrm{Re}(z_1)| \leq 1/4, \quad |z_j| \leq 1/2,\ j \geq 2$$

otherwise. In all cases $B$ is a compact centrally-symmetric convex body and $\mathrm{vol}(B) = 2^{n-r_2}|d|^{1/2}$.

By Theorem 5.3 from the lectures the volume of the fundamental region for $\Lambda = i(\mathcal{O}_K)$ is $2^{-r_2}|d|^{1/2}$. Therefore, by Minkowski's theorem there exists a non-zero $\alpha \in \mathcal{O}_K$ such that $i(\alpha) \in B$. Since $\alpha \in \mathcal{O}_K$, the absolute value of $N_{K/\mathbb{Q}}(\alpha)$ is a positive integer, i.e., $|\sigma_1(\alpha)| \prod_{j=2}^{n} |\sigma_j(\alpha)| \in \mathbb{Z}_{>0}$. By definition of $B$ we have $|\sigma_j(\alpha)| \leq 1/2$ for $j \geq 2$, and therefore $|\sigma_1(\alpha)| > 1$.

If $r_1 > 0$, this shows that $\sigma_1(\alpha) \neq \sigma_j(\alpha)$, $j \neq 1$, and thus $\alpha$ is a primitive element of $K$, i.e., $K = \mathbb{Q}(\alpha)$. Indeed, if it were not primitive, its characteristic polynomial would be equal to some power ($> 1$) of its minimal polynomial, and hence $\sigma_1(\alpha)$ would be equal to $\sigma_j(\alpha)$ for some $j \neq 1$.

If $r_1 = 0$, $\sigma_1$ is a complex embedding, and thus there is still the possibility that $\sigma_1(\alpha) = \overline{\sigma_1(\alpha)}$. However, since $|\mathrm{Re}(\sigma_1(\alpha))| \leq 1/4$ and $|\sigma_1(\alpha)| > 1$, $\sigma_1(\alpha)$ cannot be real, and thus $\sigma_1(\alpha) \neq \overline{\sigma_1(\alpha)}$. Therefore, in this case $\alpha$ is also primitive.

Finally, since $B$ is bounded, all conjugates $\sigma_j(\alpha)$ are bounded. Since the characteristic polynomial of $\alpha$ is $p(x) = \prod_{j=1}^{n}(x - \sigma_j(\alpha))$, this implies that all its coefficients are also bounded. But $p(x) \in \mathbb{Z}[x]$, so there are only finitely many possibilities for $p(x)$, and hence for $\alpha$. Since $\alpha$ is primitive, $K = \mathbb{Q}(\alpha)$ and we conclude that there are only finitely many number fields of discriminant $d$.