ÉNS Lyon
2017-2018

Number Theory
M1

Exercise sheet 6
Binary quadratic forms and midterm revisions

The exercises 4 to 7 are, with some added questions, taken from midterms and exams from the previous years.

Exercise 1. [Computation of $\mathrm{Cl}(D)$]

Using Gauss' theorem on reduced forms with negative discriminant, compute $\mathrm{Cl}(D)$ for $D = -11, -19, -20, -23, -24$.

Exercise 2. [Reduction algorithm for negative discriminant]

Let $q = (a, b, c)$ be a positive quadratic form with discriminant $D < 0$. We will here explain the algorithm to obtain its reduced form.

(a) Prove that $a > 0$ and $c > 0$.

(b) If $c < a$, use proper equivalence to reduce to the case $c \geq a$.

(c) If $|b| > a$, use proper equivalence to reduce to the case $|b| \leq a$. How does this reduction behave with respect to the hypothesis $c < a$? Does this process terminate ?

(d) Assume we obtain after proper equivalence a form with $a \leq b \leq a \leq c$. If $b = -a$, prove one can reduce to $b = a$.

(e) If $c = a$, prove one can reduce to $b \geq 0$.

(f) Reduce the forms $(3, 3, 2)$ and $(4, 5, 3)$.

Exercise 3. [Reduction of forms with square discriminants]

Let $k \in \mathbb{N}^*$ and $D = k^2$.

(a) For a form q of discriminant D, find a nontrivial solution of $q(x, y) = 0$.

(b) Deduce that $q \overset{+}{\sim} (0, k, c')$ for some $c' \in \{0, \cdots, k-1\}$.

Exercise 4. [Prime numbers represented by quadratic forms]

Consider the quadratic form $q = (8, 5, 1)$.

(a) Give the reduced positive form properly equivalent to q. Are there other reduced positive forms with the same discriminant ?

(b) Prove that every prime number $p \equiv 1 \mod 7$ is represented by q.

(c) Which other prime numbers are represented by q ?

Exercise 5. [Real cyclotomic fields]

Consider $p \geq 3$ a prime number, $\zeta_p = e^{2i\pi/p}$ and $K = \mathbb{Q}(\zeta_p)$.

(a) Prove that the family of ζ^i, $1 \leq i \leq (p-1)/2$ or $1 \leq -i \leq (p-1)/2$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

(b) Defining $F = \mathbb{Q}(\zeta_p)^+ = \{\ x \in K, \mid \overline{x} = x\}$, prove that

$$F = \mathbb{Q}(\cos(2\pi/p)).$$

(c) Prove that $\mathcal{O}_F$ is the $\mathbb{Z}$-algebra generated by $2\cos(2\pi/p)$.

(d) Write the decomposition in prime ideals of $p\mathcal{O}_F$.

Exercise 6. [A principality criterion]

Let $p \equiv 3 \mod 4$ prime and $K = \mathbb{Q}(\zeta_p)$.

(a) For $F = \mathbb{Q}(\sqrt{-p})$, recall why $F \subset K$. Prove that for $n \in \mathbb{Z}$, if $n = N_{K/\mathbb{Q}}(x)$ for some $x \in \mathcal{O}_K$, then $n = |z|^2$ for some $z \in \mathcal{O}_F$.

(b) Let $\ell \equiv 1 \mod p$ be a prime number. Prove that $\mathcal{O}_K$ contains an ideal of norm ℓ.

(c) If $\mathcal{O}_K$ is principal, deduce that ℓ is represented by the quadratic form $x^2 + xy + (1+p)/4y^2$.

(d) Prove that for $p = 23$, $\mathcal{O}_K$ is not principal.

Exercise 7. [Diophantine equations and class numbers]

Let $d < 0$ be an even squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. We assume there exists $(x, y) \in \mathbb{Z}^2$ such that

$$y^2 = x^5 + d.$$

(a) Prove that x, y are odd and coprime, and that $x \geq 3$.

(b) Prove that the ideals $(y + \sqrt{d})$ and $(y - \sqrt{d})$ are coprime.

(c) Prove that there is an ideal I of $\mathcal{O}_K$ such that $(y + \sqrt{d}) = I^5$.

(d) Assume now that $|\operatorname{Cl}(\mathcal{O}_K)|$ is not divisible by 5. Prove that there are $a, b \in \mathbb{Z}$ such that

$$\begin{aligned} a^5 + 10a^3b^2d + 5ab^4d^2 &= y, \\ 5a^4b + 10a^2b^3d + b^5d^2 &= 1. \end{aligned}$$

(e) Prove that a is odd, $b = \pm 1$ and $5a^4 + 10a^2d + b^5d^2 = \pm 1$. Reducing this equality modulo 8, deduce a contradiction, therefore 5 divides $|\operatorname{Cl}(\mathcal{O}_K)|$.

(f) Prove that for $d = -74, -194$, the class number of $\mathcal{O}_K$ is divisible by 5.

(g) Prove that the equations $y^2 = x^5 - 2$ and $y^2 = x^5 - 6$ do not have solutions $x, y \in \mathbb{Z}$.