ÉNS Lyon Number Theory
2017-2018 M1

Exercise sheet 5
Class groups and binary quadratic forms

Exercise 1. [Decomposition of prime numbers in the cyclotomic case]

Let $n \geq 3$, $\zeta_n = e^{2i\pi/n}$ and $K = \mathbb{Q}(\zeta_n)$. The minimal polynomial of ζ_n is the n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$ and the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

(a) For p prime not dividing n, describe the factorisation of Φ_n modulo p.

(b) Deduce the shape of the decomposition of $p\mathcal{O}_K$ in terms of the congruence class of p modulo n.

Exercise 2.

Let K be a number field.

(a) Prove that for every ideal I of $\mathcal{O}_K$, there is a finite extension L of K for which $I \cdot \mathcal{O}_L$ is principal.

(b) Prove that there is a finite extension L of K such that for every ideal I of $\mathcal{O}_K$, $I \cdot \mathcal{O}_L$ is principal.

Exercise 3. [Second case of Fermat's last theorem]

We assume here that $p \geq 3$ is a regular prime number, and want to show that there is no solution to the equation in integers

$$x^p + y^p = z^p$$

where $p|z$ and x, y, z are pairwise coprime.

We assume there is such a solution (x, y, z) and will derive a contradiction.

(a) We define $\zeta = e^{2i\pi/p}$. Recall why $(p) = (1-\zeta)^{p-1}$ is the decomposition of (p) into prime ideals in $\mathcal{O}_K$.

(b) Prove that p divides $x + y$ in $\mathbb{Z}$, hence that $(1-\zeta)^{p-1}$ divides $x + y$ in $\mathcal{O}_K$.

(c) Prove that $(1-\zeta)$ actually divides all the $x + \zeta^i y$ for $0 \leq i \leq p-1$.

(d) Prove that $(1-\zeta)^2$ does not divide any $x + \zeta^i y$ for $1 \leq i \leq p-1$.

(e) Obtain with the previous questions the equality of integral ideals

$$\left(\frac{z}{(1-\zeta)^{p-1}}\right)^p = \left(\frac{x+y}{(1-\zeta)^{(p-1)^2}}\right) \prod_{i=1}^{p-1} \left(\frac{x+\zeta^i y}{1-\zeta^i}\right),$$

where all the ideals on the right are pairwise coprime.

(f) Deduce, similarly as in the first case of Fermat's last theorem, that

$$x + \zeta y = (1-\zeta)\alpha^p \zeta^r v$$

with $\alpha \in \mathcal{O}_K$, $v \in \mathcal{O}_F^*$ where $F = \mathbb{Q}(\cos(2\pi/p))$ and $r \in \mathbb{Z}$.

(g) Proceeding similarly again, establish that

$$\zeta^{-r}\frac{x+\zeta y}{1-\zeta} - \zeta^{r}\frac{x+\zeta^{-1}y}{1-\zeta^{-1}} \in p\mathcal{O}_K.$$

(h) Prove that

$$\frac{p}{1-\zeta} = 1 + \sum_{i=1}^{p-2}(p-1-i)\zeta^i$$

and

$$\frac{p}{1-\zeta^{-1}} = 1 + \sum_{i=1}^{p-2}(i+2-p)\zeta^i.$$

(i) Write $(x+\zeta y)/(1-\zeta)$ and $(x+\zeta^{-1}y)/(1-\zeta^{-1})$ using the previous formulas. Separating between the cases $p^2|x+y$ and $p^2 \nmid x+y$, find a contradiction.

Exercise 4. [Primitive forms and fundamental discriminants]

A quadratic form $q(x,y) = ax^2+bxy+cy^2$ is *primitive* if $\gcd(a,b,c) = 1$. An integer $D \equiv 0,1 \mod 4$ is a *fundamental discriminant* if every form with disriminant D is primitive.

(a) Prove that for every D, the quadratic form q_D is primitive.

(b) If $D \equiv 1 \mod 4$, prove that D is a fundamental discriminant if and only if it is squarefree.

(c) If $D \equiv 0 \mod 4$, prove that D is a fundamental discriminant if and only if $D/4 \equiv 2,3 \mod 4$ and $D/4$ is squarefree.

Exercise 5. [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 $c' \in \{0,\cdots,k-1\}$.