Avertissement.

Cette rédaction est destinée aux étudiants qui ont suivi mon cours de Théorie des Nombres durant l'année 1967-1968.

Les §§ 1 à 6 n'y sont pas inclus. Comme on voit par le sommaire, ils concernent la théorie élémentaire des nombres rationnels. Le contenu peut se trouver dans mon cours de 1958-59 rédigé par P. Besson, et dans d'excellents ouvrages, par exemple celui de Davenport cité § 23 ou celui de Hardy & Wright cité § 28.

Lausanne, septembre 1968

G. de Rham

Cours de Théorie des Nombres 1967-68

de Rham

Sommaire

§1. Rappel des notions d'anneau, idéal, anneau quotient, homomorphisme d'anneau. L'anneau $\mathbb{Z}$, lemme d'Euclide, nombres premiers, théorème fondamental de l'arithmétique.

§2. Les équations $x^2+y^2=z^2$ et $x^4+y^4=z^2$.

§3. Anneau intègre, idéal premier, groupe des unités, corps. Anneau principal (= anneau intègre où tout idéal est principal). Factorisation dans un anneau principal. L'anneau $K[x]$, où K est un corps. Polynomes primitifs. Théorème de Gauss et critère d'irréductibilité d'Eisenstein.

§4. L'indicateur d'Euler $\varphi(n)$ et les unités de $\mathbb{Z}/(n)$. L'isomorphisme $\mathbb{Z}/(ab) \simeq \mathbb{Z}/(a) \times \mathbb{Z}/(b)$ pour $(a,b)=1$. Existence de racines primitives (mod p).

§5. Numération de base a. Fractions décimales périodiques.

§6. Résidus quadratiques. Symbole de Legendre. Critère d'Euler. Loi de réciprocité. Lemme de Gauss. Symbole de Jacobi.

§7. Les entiers d'un corps quadratique. Les unités. Méthode de Dirichlet pour prouver l'existence de l'unité fondamentale dans un corps réel.

§8. Corps quadratiques euclidiens. Factorisation. Entiers de Gauss et nombre de solutions de $x^2+y^2=n$. $Q(\sqrt{m})$ pour $m = -1, -3, -2, 2$. Cas de $Q(\sqrt{-5})$.

§9. Les idéaux de l'anneau des entiers d'un corps quadratique et leur décomposition en facteurs premiers. [Le lemme : $\mathfrak{a}\mathfrak{a}'$ = idéal principal rationnel.].

§10. Congruences. Norme des idéaux. Les théorèmes $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}.N\mathfrak{b}$, $\varphi(\mathfrak{a}) = N\mathfrak{a} \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N\mathfrak{p}}\right)$, $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$.

§11. Les idéaux premiers d'un corps quadratique. Le caractère $\chi(x)$ d'un corps quadratique.

§12. Classes d'idéaux. Idéaux fractionnaires.

Finitude du nombre des classes, classes au sens restreint.

§13. Formes quadratiques binaires. Equivalence propre ou impropre. Relation entre les classes d'idéaux (au sens restreint) du corps de discriminant D et les formes quadratiques de même discriminant.

§14. Groupe modulaire. Points rationnels proches, suites de Farey. Le domaine fondamental Δ.

§15. Réduction des formes quadratiques binaires.

Deux formes primitives sont (proprement) équivalentes si et seulement si leurs premières racines sont équivalentes. Elles sont improprement équivalentes si et seulement si la 1ère racine de l'une est improprement équivalente à la 2ème racine de l'autre.

Formes réduites définies positives (la première racine est dans Δ) et indéfinies (la première racine est > 1 et la 2-ième est entre -1 et 0.