ALGEBRAIC NUMBER THEORY-SUMMER SCHOOL NOTES

Contents

1. Lecture 1: July 30: Introduction

1.1. Diophantine equation.

Example 1.1. Consider the equation

$$x^2 + y^2 = 1$$

in the rational number eld $\mathbb{Q}$.

We know that (1; 00509 0 Td [(;)]TJ/F88

1.2. Algebraic Integers.

Definition 1.9. Let $A \subset B$ be an extension of rings. $x \in B$ is called *integral* over A if x satisfies

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$. B is *integral* over A if all $x \in B$

Here non-degenerate means that if $\mathrm{Tr}_{L/K}(xy) = 0$ for all $y \in L$, then $x = 0.$ Or equivalently to say, $L \simeq \mathrm{Hom}_K(L; K)$ induced by $\mathrm{Tr}_{L/K}$.

1.4. Exercise Sheet 1.

Exercise 1.

3. Lecture 3: August 2

3.1. **Dedekind domain.** A is called a Dedekind domain if A is Noetherian, integrally closed and each nonzero prime ideal is maximal.

Note that localization of a Dedekind domain is also Dedekind. We always have the following setting in this section. Let A be a Dedekind domain, let K be the fractional eld of A. Let $L=K$ be a nite separable extension. Let B be the integral closure of A in L.

Proposition 3.1. *Let A be a Dedekind domain, let K be the fractional eld of A. Let $L=K$ be a nite separable extension. Let B be the integral closure of A in L. Then B is a Dedekind domain.*

Proof. Of course B is integrally closed. Let $P A$

Remark 3.8. There are Dedekind domain A s.t. Cl_A is in nite.

Example 3.9. $A = \mathbb{C}[x; y]=(y^2$

(1) p rami ed in K, i.e. some $e_i > 1$, i

$$p \; j \quad _K = \quad 4d \quad d \quad 2;$$

4. Lecture 4: August 5

Let L/K be a nite extension of number elds with integer ring B and A, and $\mathfrak{p} \neq 0$ be a prime of $\mathcal{O}_K$. We have a prime decomposition

$$\mathfrak{p}$$

4.4. Exercise sheet 4.

Exercise 1. *Use the cyclotomic extension* $\mathbb{Q}(\ _8)$ *to show the quadratic reciprocity law for* 2*: if* p *is an*

5. Lecture 5: August 6

Let K be a number field and

$$\mathrm{Cl}_K = I_{O_K}/P_{O_K}$$

where I_{O_K} is the free group generated by fractional ideals of O_K with P_{O_K} the subgroup consisting of principal fractional ideals.

Theorem 5.1.

Note that for any number eld K, the Minkowski constant C_K

Theorem 5.11. *For a number eld K, there exists a unique nite extension*

6. Lecture 6: August 9

6.1.

Theorem 6.11 (Iwasawa). *Let $K_1 = K$ be a Z_p*

Let $\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} =: V$, V is a $\mathbb{R}$-algebra, and $V^{\times} = (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}$. For any element $(y_i; z_j) \in V^{\times}$, define norm to be $N(y_i; z_j) = \prod_i |y_i| \prod_j |z_j|^2$. Then for any $\alpha \in O_K$, $\Rightarrow$

6.3. Exercise sheet 6.

Exercise 1. *The aim of this exercise is to give a proof of the niteness of the ideal class group of a number eld K*