Student seminar notes week 1

Dimitri Wyss

1 Recollection on number and local fields

In this sections we recall some basic facts about number fields and their completions.

1.1 Number fields

A *number field* F is a finite extension of the rational numbers $\mathbb{Q}$. The integral closure $\mathcal{O}_F$ of $\mathbb{Z}$ inside F is called *the ring of integers* of F.
While $\mathcal{O}_F$ fails in general to be a PID or a UFD, it has the structure of a Dedekind domain i.e. it's a Noetherian, integrally closed domain and every non-zero prime ideal is maximal. As a consequence any ideal in $\mathcal{O}_F$ admits a unique factorization into prime ideals. Hence it make sense to write $\mathfrak{p}|\mathfrak{a}$ whenever $\mathfrak{p}$ is a factor in the decomposition of an ideal $\mathfrak{a} \subset \mathcal{O}_F$.

Example 1.1. In $\mathbb{Z}[\sqrt{-5}]$ we have

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

two factorizations into irreducibles. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. But the ideal (6) factors uniquely as $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$. Notice that (2) and (3) are not prime ideals since for example $(1+\sqrt{-5})(1-\sqrt{-5}) \in (3)$ but neither $(1+\sqrt{-5}) \notin (3)$ and similarly for (2).

A *fractional ideal* of F is a non-zero finitely generated $\mathcal{O}_F$-submodule of F. The set of fractional ideals form an abelian group $\mathcal{I}_F$ under multiplication with identity $\mathcal{O}_F$ and for any $\mathfrak{a} \in \mathcal{I}_F$ its inverse is given by

$$\mathfrak{a}^{-1} = \{x \in F \mid x\mathfrak{a} \subset \mathcal{O}_F\}.$$

It follows from the unique factorization of any ideal into prime ideals, that $\mathcal{I}_F$ is the free abelian group generated by the non-zero prime ideals of $\mathcal{O}_F$.

Example 1.2. Any fractional ideal in $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Q}^\times$. Its inverse is given by $a^{-1}\mathbb{Z}$.

A fractional ideal is *principal* if it's generated by a single element in $F^\times$. Principal fractional ideals form a subgroup $\mathcal{P}_F \subset \mathcal{I}_F$ and the *ideal class group* of F is the quotient

$$\mathcal{C}_F = \mathcal{I}_F / \mathcal{P}_F.$$

One of the first non-trivial theorems in algebraic number theory states that $\mathcal{C}_F$ is a fintie group for any number field F. The *class number* h_F of F is the order of $\mathcal{C}_F$. Essentially by definition $h_F = 1$ if and only if $\mathcal{O}_F$ is a PID.

Given an extension K/F of number fields and an ideal $\mathfrak{p} \subset \mathcal{O}_F$ we may consider the unique factorization of $\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K$:

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Here $\mathfrak{P}_i$ are distinct prime ideals in $\mathcal{O}_K$ and $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ is the *ramification index* of $\mathfrak{P}_i/\mathfrak{p}$.