# Part III Algebraic Number Theory
2014

Part III Algebraic Number Theory 2014

# Contents

# Chapter 1

# Dedekind domains

## 1.1 Introduction

These are lecture notes for the 2014 Part III Algebraic Number Theory course taught by Dr. Jack Thorne, these notes are part of Mjolnir.

The recommended books are:

- H. P. F. Swinnerton-Dyer - A Brief Guide to Algebraic Number Theory
- Serge Lang - Algebraic Number Theory

Generated: May 21, 2015, 07:04:50 (Z)

## 1.2 Basics

**Definition 1.2.1** (Number fields)**.** A **number field**$K$ is a finite degree field extension of $\mathbf{Q}$.

**Definition 1.2.2** (Integral elements)**.** If $K$ is a number field and $\alpha \in K$ then we say $\alpha$ is **integral** if there exists a $f \in \mathbf{Z}[x]$ monic with $f(\alpha) = 0$.

If $\alpha$ is integral than $\mathbf{Z}[\alpha] \subset K$ is finitely generated. Conversely if $\alpha \in K$ and $\mathbf{Z}[\alpha]$ is a finitely generated $\mathbf{Z}$-module then $\alpha$ is integral over $K$. (If $\mathbf{Z}[\alpha]$ is spanned by $f_1(\alpha), \dots, f_k(\alpha)$ $f_i \in \mathbf{Z}[x]$ then for any $n > \max \deg f_i$ we can write $\alpha^n = \sum_{i=1}^k a_i f_i(\alpha)$ for some $\alpha_i \in \mathbf{Z}$. This implies that $\alpha$ is a zero of $x^n - \sum_{i=1}^k a_i f_i(x) \in \mathbf{Z}[x]$. We have shown that if $\alpha, \beta \in K$ are integral over $\mathbf{Z}$ then so are $\alpha \pm \beta$ and $\alpha\beta$ (as it is easy to see $\mathbf{Z}[\alpha, \beta]$ is a finitely generated $\mathbf{Z}$-module).)

**Definition 1.2.3** (Rings of integers)**.** If $K$ is a number field let $\mathcal{O}_K$ be the **ring of integers**, defined by

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ integral over } \mathbf{Z}\}.$$

This is the integral closure of $\mathbf{Z}$ in $K$.

## 1.3 Dedekind domains

Let $R$ be an integral domain, $K = \mathrm{Frac}(R)$.

**Definition 1.3.1** (Dedekind domains)**.** We then say that $R$ is a **dedekind domain** if it is

1. Noetherian,
2. integrally closed in $K$,
3. and in it every non-zero prime is maximal.

**Exercise 1.3.2.** Show that every PID is a dedekind domain.

**Definition 1.3.3** (Fractional ideals)**.** If $R$ is a dedekind domain we call every finitely generated $R$-submodule of $K$ a fractional ideal.

This definition includes ideals $I \subset R$.

**Proposition 1.3.4.** *Let $R$ be a dedekind domain and let $\mathcal{I}$ be the set of non-zero fractional ideals of $R$, then $\mathcal{I}$ is a group under multiplication.*

*Proof.* We deonte ideals of $R$ by $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subset R$ and (non-zero) prime ideals by $\mathfrak{p}, \mathfrak{q}, \mathfrak{r} \subset R$. Multiplication is given by

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_i : a_i \in \mathfrak{a},\, b_i \in \mathfrak{b} \right\}.$$

Then the identity for this operation is $(1) = R$. The key part of this proof is the construction of inverses.

**Claim 1.3.5.** *For any non-zero ideal $\mathfrak{a} \subset R$ there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_m \subset \mathfrak{a}$.*

*Proof.* Suppose not, then we can find an $\mathfrak{a} \subset R$ which is maximal among such ideals having this property (as $R$ is noetherian). Then $\mathfrak{a}$ is not prime, as otherwise the claim is clearly true, so there exists some $\alpha, \beta \in R$ with $\alpha\beta \in \mathfrak{a}$ but $\alpha, \beta \notin \mathfrak{a}$. So we have that $\mathfrak{a} \subsetneq \mathfrak{a} + (\alpha)$ and $\mathfrak{a} \subsetneq \mathfrak{a} + (\beta)$. By the maximality of $\mathfrak{a}$ we can find $\mathfrak{p}_1 \cdots \mathfrak{p}_m \subseteq \mathfrak{a} + (\alpha)$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq \mathfrak{a} + (\beta)$ but now

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq (\mathfrak{a} + (\alpha))(\mathfrak{a} + (\beta)) \subseteq \mathfrak{a} + (\alpha\beta) \subseteq \mathfrak{a},$$

contradiction. □

**Claim 1.3.6.** *For any non-zero prime ideal $\mathfrak{p} \subset R$ there exists $\delta \in K \setminus R$ such that $\delta\mathfrak{p} \subseteq R$.*

*Proof.* Choose $\beta \in \mathfrak{p} \setminus \{0\}$ and an expression $\mathfrak{p}_1 \cdots \mathfrak{p}_m \subseteq (\beta)$ with $\mathfrak{p}_i$ non-zero prime ideals and $m$ minimal. Then there exists $i$ such that $\mathfrak{p}_i \subset R$ otherwise for all $i$ there is some $\alpha_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, in which case $\alpha_1 \cdots \alpha_m \in \mathfrak{p}_1 \cdots \mathfrak{p}_m \subseteq (\beta) \subseteq \mathfrak{p}$, a contradiction □

□