School of Mathematical Sciences
PURE MTH 3007
Groups and Rings III, Semester 1, 2009

Week 11 Summary

Week 11 — Lecture 25 — Tuesday 26th May.

12.2.1. *The integral domains* $\mathbb{Z}(\sqrt{d})$. **The Gaussian integers** This is the integral domain

$$\mathbb{Z}(i) = \{m + ni \mid m, n \in \mathbb{Z}\}$$

with $\delta(m + ni) = m^2 + n^2$ and $i = -1$ as usual. Then δ is a Euclidean valuation.

The general case If $d \in \mathbb{Z}$ we define

$$\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

This is an integral domain, a subdomain of $\mathbb{C}$. We normally take $d \neq 0, 1$ and d squarefree.

The *norm* in $\mathbb{Z}(\sqrt{d})$ is the function $N : \mathbb{Z}(\sqrt{d}) \to \mathbb{N}$ given by

$$N(a + b\sqrt{d}) = |a^2 - db^2|.$$

Theorem 12.3. *In* $\mathbb{Z}(\sqrt{d})$,

(i) $N(x) = 0$ *if and only if* $x = 0$
(ii) *for all* $x, y \in \mathbb{Z}(\sqrt{d})$, $N(xy) = N(x)N(y)$
(iii) x *is a unit if and only if* $N(x) = 1$
(iv) *if* $N(x)$ *is prime, then* x *is irreducible in* $\mathbb{Z}(\sqrt{d})$.

Note that N is in some cases, but not in all cases, a Euclidean valuation, so for some d, $\mathbb{Z}(\sqrt{d})$ is a Euclidean domain.

Week 11 — Lecture 26 — Wednesday 27th May.

12.3. **Principal ideal domains.**

Definition 12.4. An integral domain D is a *principal ideal domain (PID)* if every ideal of D is principal.

Theorem 12.5. *Every Euclidean domain is a PID.*

Examples:

(1) $\mathbb{Z}$ is an ED and hence a PID.
(2) If F is a field, $F[x]$ is an ED, and hence a PID.
(3) The Gaussian integers $\mathbb{Z}(i)$ is a PID.
(4) The domain $\mathbb{Z}[x]$ is *not* a PID. (Consider the ideal $\langle 2, x\rangle = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$.)

Week 11 — Lecture 27 — Friday 29th May.

13. Unique Factorization Domains

13.1. Definitions.

Definition 13.1. An integral domain D is called a *unique factorization domain (UFD)* if for every $a \in D$, not zero or a unit,

(i) $a = c_1 c_2 \dots c_n$ for irreducibles c_i
(ii) if $a = c_1 c_2 \dots c_n = d_1 d_2 \dots d_m$ with c_i, d_j all irreducible then $n = m$ and the d_i can be renumbered such that each c_i is an associate of d_i.

13.2. Irreducibility tests for polynomials.

Lemma 13.2. *Let F be a field. If $f(x) \in F[x]$ has degree 2 or 3 then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Theorem 13.3 (Eisenstein's criterion)**.** *Let $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$. Suppose that there is a prime p such that*

(i) $p \not| a_n$
(ii) $p | a_i$ *for* $i = 0, 1, \dots, n-1$
(iii) $p^2 \not| a_0$.

Then apart from a constant factor $f(x)$ is irreducible over $\mathbb{Z}$.

13.3. Irreducibles and primes.

Definition 13.4. Let a, b elements of an integral domain D. If $a \neq 0$ we say that a *divides* b ($a \mid b$) if $b = ac$ for some $c \in D$.

Definition 13.5. An element p of an integral domain D, not zero or a unit, is called *prime* if whenever $p | ab$ for $a, b \in D$, either $p | a$ or $p | b$.

Lemma 13.6. *Every prime in an integral domain is irreducible.*

Theorem 13.7. *Let D be an integral domain. Then D is a UFD if and only if*

(i) *for every $a \in D$, not zero or a unit, $a = c_1 c_2 \dots c_n$ for irreducibles c_i*
(ii) *every irreducible in D is prime.*

Theorem 13.8. *Every PID is a UFD.*