35003 MODERN ALGEBRA

Prof Murray Elder, UTS

Week 9: Field of fractions; Unique Factorisation Domains

Lauritzen 3.4–3.5

Exercise: let p be a prime and $a, b \in \mathbb{Z}$.

If $p \mid ab$ then $p \mid a$ or $p \mid b$ for any $a, b \in \mathbb{Z}$.

Prove this without resorting to writing out prime factorisations.

Proof: Suppose $p \mid ab$ and p does not divide a. Then $\gcd(a, p) = 1$ so $1 = \lambda p + \mu a$ for some $\lambda, \mu \in \mathbb{Z}$.

Then multiply by b:

$$b = \lambda pb + \mu ab$$

so p divides the RHS so $p \mid b$. $\square$

For the rest of this chapter of Lauritzen (3.4 and 3.5) R is a domain.

Define an equivalence relation on $M = R \times (R \setminus \{0\}$ by $(a, s) \sim (b, t)$ if $at = bs$ in the ring.

Write an element of the equivalence class of a pair (a, s) as $\frac{a}{s}$

Let $Q = M/\sim$ and define addition and multiplication by

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \quad \text{and} \quad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

with $\frac{0}{s}$ the zero element and $\frac{s}{s}$ the 1 element.

If $\frac{a}{s} \neq 0$ then $a \neq 0$ so we can write $\frac{s}{a} \in Q$ and multiply them together gives 1, so Q is a field.

We also have an injective ring homomorphism $\iota\colon R \to Q$ defined by $\iota(a) = \frac{a}{1}$.

Q is "the smallest field containing R" in the following sense.

Proposition (3.4.1)

Let R be a domain with Q the field of fractions obtained on the previous slide.

Let L be a field and $\varphi\colon R \to L$ an injective ring homomorphism.

Then there is a unique injective ring homomorphism $\tilde{\varphi}\colon Q \to L$ such that $\tilde{\varphi} \circ i = \varphi$.

Corollary (3.4.2)

Let R be a domain contained in a field L. The smallest subfield in L containing R is

$$K = \{as^{-1} \mid a \in R, s \in R \setminus \{0\}\}$$

(where $s^{-1} \in L$ since L is a field; s^{-1} might not live in $R \setminus \{0\}$)

and the field of fractions of R is isomorphic to K.

See Lauritzen for the proofs of these, or try yourself.

Eg: the Gaussian integers $\mathbb{Z}[i]$ has field of fractions isomorphic to $\mathbb{Q}(i)$.

We continue to assume R is a domain.

Let $x, y \in R$. If $x = ry$ for some $r \in R$ then we say y divides x, y is a divisor of x, $y \mid x$.

Ex: $y \mid x$ if and only if $\langle x \rangle \subseteq \langle y \rangle$

If $x = uy$ and u is a unit, then the ideals generated by x and y are the same.

Conversely, suppose $\langle x \rangle = \langle y \rangle$. Then $x = ry$ and $y = sx$ for some $r, s \in R$. So

$$1x = x = ry = r(sx) = (rs)x$$

and we are in a domain, so $rs = 1$ (Proposition 3.1.3 from last week).

Thus $r, s \in R^*$. So we have proved

$$\langle x \rangle = \langle y \rangle \quad \text{if and only if} \quad \exists u \in R^* [x = uy]$$

An element $d \in R$ is called a *greatest common divisor* of $a, b \in R$ if d is a divisor of each and every other common divisor divides d ($\forall c$ if $c \mid a$ and $c \mid b$ then $c \mid d$).

(This is the same as the defn of gcd for integers)

Let R be a PID (every ideal is principle: generated by a single element)

For each $a, b \in R$ the ideal $\langle a, b \rangle = \{\lambda_1 a + \lambda_2 b \mid \lambda_1, \lambda_2 \in R\}$ must be generated by a single element, so

$$\langle a, b \rangle = \langle d \rangle$$

for some $d \in R$.

Ex: the generator d is the greatest common divisor of a, b.

An element $r \in R \setminus R^*$ is called *irreducible* if $r = ab$ for $a, b \in R$ implies either a or b is a unit.

Its a bit like being a prime number in the integers: $p \in \mathbb{Z}$ is a prime if $p = ab$ means one of a, b has to be ± 1.

Ex: If r is irreducible and $u \in R^*$ then ur is irreducible.

A non-zero, non-unit element $x \in R$ is said to have a factorisation into irreducible elements if there exist irreducible elements $p_1, \ldots, p_r$ so that

$$x = p_1 \cdots p_r$$

Of course this is not unique if R^* has more than 1 in it.

We say it is "unique" if for any other factorisation into irreducible elements

$$x = q_1 \ldots q_s$$

every p_i divides some q_j (so $p_i = uq_j$ for some unit $u \in R^*$)

Then

$$p_1 \ldots p_r = u_{j_1} q_{j_1} \cdots u_{j_r} q_{j_r} = q_1 \ldots q_s$$

and we are in a (commutative) domain so one-by-one apply Prop 3.1.3 to cancel the q_{j_k} with q_i, to get $r = s$.

Definition

A domain where every non-zero, non-unit element has a unique factorisation into irreducible elements is called a UFD.

Eg: in the domain $\mathbb{Z}$, the irreducible elements are $\pm p$ where p is prime. Every element has a unique factorisation into primes (with ± 1 out the front) so $\mathbb{Z}$ is a UFD.

Recall the exercise we did about prime numbers in $\mathbb{Z}$ at the start of the lecture.

Definition

A non-zero element $p \in R \setminus R^*$ is called a *prime element* of the domain R if

$$p \mid xy \text{ implies } p \mid x \text{ or } p \mid y$$

where $x, y \in R$.

Proposition (3.5.2)

A prime element is irreducible.

Proof: Let p be a prime (non-zero non-unit).

Suppose $p = xy$.

We want to show that one of x, y is a unit.

We know from defn of prime that $p \mid x$ or $p \mid y$ so assume $p \mid x$.

Then $x = pr$ for some $r \in R$.

Then $p = xy = pry$ so Prop 3.1.3 (we are in a domain) says $1 = ry$, so y is a unit. $\square$

Proposition (3.5.3 (Technical Lemma))

Let R be a domain for which every non-zero non-unit element has a factorisation into irreducible elements.

Every irreducible element is a prime element iff R is a UFD.

Proof: Suppose every irreducible element is a prime.

And suppose some element has two irreducible factorisations

$$p_1 \cdots p_r = q_1 \cdots q_s$$

For each irreducible p_i, we have p_i divides $q_1(q_2 \ldots q_s)$. So by definition of prime (since p_i is also prime) p_i divides q_1 or the rest. Repeat until you find q_j that p_i divides.

Thus every p_i divides some q_j.

If R is a UFD, and let p be irreducible.

Suppose $p \mid xy$. If $xy = 0$ then we are in a domain so one of $x, y = 0$ so we are done. Else $x, y, xy \neq 0$.

Let r be such that $rp = xy$. We are in a UFD so x, y, r all have factorisations into irreducible elements $q_1 \cdots q_\ell$, $t_1 \cdots t_s$, $r = r_1 \cdots r_m$ so

$$r_1 \cdots r_m p = q_1 \cdots q_r t_1 \cdots t_s$$

where every letter here is an irreducible element.

By uniqueness, we have p must divide one of the q_i or t_j

so p divides x or y

$\mathbb{Z}[\sqrt{-5}]$ is a domain where

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

To show $\mathbb{Z}[\sqrt{-5}]$ is not a UFD we need to show that $2, 3, 1 \pm \sqrt{-5}$ are all irreducible and say 2 does not divide $1 \pm \sqrt{-5}$.

Or by the previous proposition it is enough to show one element, say 2 is irreducible but not prime.

Ex: do this (see top of page 128 Lauritzen for steps).

Lemma (3.5.5)

Let R be a PID and $0 \neq r \in R \setminus R*$. Then r has an irreducible factorisation.

Proof: Suppose r is not a product of irreducible elements.

Then r is not irreducible itself, so $r = r_1 s_1$ where neither are units, and they are not both products of irreducibles (if they both are, then so was r).

Pick one of them, say r_1, is not a product of irreducible elements.

We have $\langle r \rangle \subsetneq \langle r_1 \rangle$.

Now r_1 is not a product of irreducibles so repeat: find $r_2, r_3, \ldots$ and

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_2 \rangle \ldots$$

Ex: 3.6.9: Given an increasing sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots$, then $\bigcup_{i=1}^{\infty} I_i$ is an ideal.

(And this is not true if you just have two ideals)

Ex 3.6.10: In a noetherian ring (see exercise for definition; includes PIDs) an increasing sequence of ideals must stablise: there is some N so that $I_N = I_{N+1}$.

But if r is not a product of irreducibles we can build an increasing sequence that doesn't stabilise: contradiction. $\square$

Recall: an ideal is maximal if $I \subsetneq J \subseteq R$ implies $J = R$.

Proposition (3.5.6)

Let R be a PID that is not a field.

An ideal $\langle x \rangle \subseteq R$ is maximal iff x is irreducible.

Proof: Suppose x is irreducible, and $\langle x \rangle \subsetneq J \subseteq R$ for some ideal J. We are in a PID so $J = \langle y \rangle$.

Then $x \in J$ means $x = \lambda y$. But x is irreducible so one of λ, y are a unit. If y is a unit, $J = R$. If λ is a unit, $J = \langle x \rangle$ (which its not) so $\langle x \rangle$ is a max ideal.

Now assume $\langle x \rangle$ is maximal, and $x = pq$ for some $p, q \in R$. If neither p, q are units then

$$\langle x \rangle \subsetneq \langle p \rangle \neq R.$$

Theorem (3.5.7)

If R is a PID then it is a UFD.

Proof: We already showed every non-zero, non-unit element of a PID has an irreducible factorisation.

So we just need to show it is unique.

We also showed that in a domain where every $0 \neq x \in R \setminus R^*$ has an irreducible factorisation, if every irreducible element is prime, then R is a UFD.

So we just need to show that every irreducible is prime.

Let $\pi \in R$ be an irreducible element, and $\pi \mid ab$ but $\pi \not| a$.

We showed that in a PID the ideal generated by an irreducible element is maximal. So $\langle \pi \rangle$ is maximal.

$\langle \pi, a \rangle$ is strictly bigger than $\langle \pi \rangle$, so it is all of $R = \langle 1 \rangle$.

Thus $1 = x\pi + ya$.

Multiply both sides by b: $b = xb\pi + yab$ so π divides b. $\square$

$\mathbb{Z}[\sqrt{-5}]$ is not a UFD, so it can't be a PID.

Lauritzen shows explicitly that $I = \langle 2, 1 + \sqrt{5} \rangle$ is not principal (we will go through this example in the workshop).

EUCLIDEAN DOMAIN

Recall the division algorithm to compute the remainder and the Euclidean algorithm to compute the gcd of two integers.

We can generalise these to domains (other than $\mathbb{Z}$) as follows.

A domain R is called a Euclidean domain if there exists a Euclidean function, which is a map

$$N\colon R \setminus \{0\} \to \mathbb{N}$$

which satisfies

for every $x \in R, d \in R \setminus \{0\}$ there exists $q, r \in R$ so that $x = qd + r$ and $r = 0$ or $N(r) < N(d)$.

For $\mathbb{Z}$, the function N is just the absolute value of the number. Take a guess (from Lauritzen's notation) what it might be for $\mathbb{Z}[i]$.

Proposition (3.5.9)

An ED is a PID.

Proof: Let $I \subset R$ be a non-zero ideal and $x \in I$ a non-zero element so that $N(x)$ is minimal (using Well Ordering Principle) compared with all other non-zero elements of I.

We will show that $I = \langle x \rangle$.

Let $y \in I$, then by definition of Euclidean function, $y = qx + r$ for $q, r \in R$ with $r = 0$ (good, then $y \in \langle x \rangle$)

or $N(r) < N(x)$.

But $y, x \in I$ means $y - qx \in I$ so $r \in I$, and x was supposed to be the smallest value. $\square$

The rest of Chapter 3 Lauritzen is some interesting Number Theory applications of ED, PID and UFDs.

Eg:

- If a prime number p is congruent to 1 mod 4, then $p = a^2 + b^2$ for a unique pair of integers a, b
- There are infinitely many primes congruent to 1 mod 4.

We will cover some of this in the workshop.

NEXT:

Friday: workshop doing more Lauritzen 3.6 exercises

- Week 10: Polynomial rings. Seminar report due this week
- Week 11: more polynomial rings (sketch of classification of finite fields)
- Week 12: final assessment (1B) in class