§1.1: Euclidean domains / PIDs.

Meet Steves.

Norms:

A norm on an int domain R is a fn $N: R \to \mathbb{Z}_{\geq 0}$ (w) $N(0)=0$ "size" of elts of R.

If $N(a)>0$ for $a \neq 0$, N is a positive norm.

Def An int. domain R is a Euclidean Domain if $\exists$ a norm N on R s.t. $\forall a, b \in R$, $b \neq 0$, $\exists q, r \in R$

$$a = qb + r, \quad r = 0 \text{ or } N(r) < N(b).$$

(q: quotient, r: remainder.)

Can repeat and get a Euclidean algorithm.

$$a = q_0 b + r_0$$
$$b = q_1 r_0 + r_1$$
$$r_0 = q_2 r_1 + r_2$$
$$\vdots$$
$$r_{n-1} = q_{n-1} r_n$$

As $N(b) > N(r_0) > \cdots > N(r_n)$ so eventually N stops decreasing.

Ex: $\mathbb{Z}$ with $N(a) = |a|$.

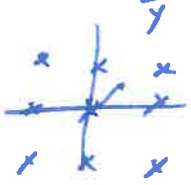
- Fields: $a = qb + 0$, $q = a/b$ (take any norm!)
- $F[x]$ for a field F. $N(p(x)) = \deg(p(x))$
  division alg. = long division of polys.
- Gaussian ints. $\mathbb{Z}[i]$ $N(r) = |r|^2$ i.e. $N(a+bi) = a^2 + b^2$.

want: given 2 elts x, y, $y \neq 0$, want q, r s.t.

$x = qy + r$, where $|r| < |y|$

$\frac{x}{y} = q + \frac{r}{y}$, $\left|\frac{r}{y}\right| < 1$.

Norm is multiplicative!

Lattice: 

given any pt in $\mathbb{C}$, at most $\frac{\sqrt{2}}{2} < 1$ away from a lattice pt q.

So $\left|\frac{x}{y} - q\right| < 1$, and so we $r = \left(\frac{x}{y} - q\right) \cdot y$ works.

Not true for other fields like $\mathbb{Q}(\sqrt{-5})$ (or else F.L.T.) $\mathbb{Z}$!

Prop: Ideals in Euc. dom. are principal.

Pf: If $I = (0)$, trivial. If $I \neq (0)$, Let $d \in I \setminus \{0\}$ be of minimum norm (by well-ordering prop).

we claim $(d) = I$.

Then $(d) \subseteq I$ (as $d \in I$).

Of course.

Conversely, $\forall\, a \in I$, divide:

$a = qd + r$, $r = 0$ or $N(r) < N(d)$.

$\Rightarrow r = a - qd$, $a \in I$, $qd \in I \Rightarrow r \in I$.

By the minimality assumption, $r = 0 \Rightarrow a = qd \in (d)$

$\Rightarrow I = (d)$!

Ex: we saw $(2, x)$ isn't principal $\Rightarrow \mathbb{Z}[x]$ isn't Euclidean. ($\exists$! a nice norm!). Note: $\mathbb{Q}[x]$ is.

gcds in [redacted].

Def: R comm. ring, $a, b \in R$, $b \neq 0$.

1). a is a multiple of b if $\exists\, x \in R$, $a = bx$. Also write $b \mid a$ (b divides a).

2). A gcd of a, b is a non-zero d s.t.

i). $d \mid a, d \mid b$, ii). if $d' \mid a, d' \mid b$, then $d' \mid d$. Denote: $\gcd(a, b)$.

e.: $b \mid a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subseteq (b)$.

Def² $I = (a,b)$ ideal gen. by a and b. $d = \gcd(a,b)$ if

i) $I \subseteq (d)$

ii) If $(d') \supseteq I \Rightarrow (d) \subseteq (d')$.

e.- $\gcd(a,b)$ is the gen of the unique smallest princ. ideal cont. a, b if it exists.

discussion

$\Rightarrow$) **Lemma** : If $(a,b) = (d)$ is principal, then $d = \gcd(a,b)$.

R int. domain

Prop: If $(d) = (d')$, then $d' = ud$, $u \in R^\times$.

In part, gcds. differ by units. (associates)

gcd a,b

Pf: Assume $d, d' \neq 0$ (or else easy)

As $d \in (d') \Rightarrow \exists x \in R$, $d = xd'$. As $d' \in (d)$,

$\exists y \in R$, $d' = xd \Rightarrow d = xyd \Rightarrow d(1-xy) = 0$. As $d \neq 0$,

$xy = 1 \Rightarrow x, y$ are units. (R an int. domain)

Th² R Euclidean domain, $a, b \in R$ non zero.

$d = r_n$ the non-zero remainder in Eucl. Alg. below.

1). $d = \gcd(a,b)$.

2). $(a,b) = (d)$ $(\Rightarrow \exists x, y \in R,\ d = ax + by)$.

Pf: (a,b) is principal as R is Eucl. Suffices to show $d = r_n$ generates (a,b), i.e.,

1). $d \mid a$, $d \mid b$ $(\Rightarrow (a,b) \subseteq (d))$

2). d is an R-lin. comb of a, b $(\Rightarrow (d) \subseteq (a,b))$.

~~To show~~ 1). Follow thru Euc. Algs

last eq^n: $r_{n-1} = q_{n-1} r_n \Rightarrow r_n | r_{n-1}$. Of course, $r_n | r_n$.

Induction (k+1)st eq^n: $r_{k-1} = q_{k+1} r_k + r_{k+1} \Rightarrow r_n | r_{k-1}$

$r_n | r_k$ $r_k | r_{k+1}$

$\Rightarrow \cdots r_n | r_1, r_0$

$\cdots \sim b = q_1 r_0 + r_1 \Rightarrow r_n | b$

$a = q_0 b + r_0 \Rightarrow r_n | a$.

2). Eq^n (0): $a = q_0 b + r_0 \Rightarrow r_0 \in (a,b)$.

(1): $r_1 = b - q_1 r_0 \in (b, r_0) \subseteq (a,b)$

$\Rightarrow \cdots \Rightarrow r_{k+1} = r_{k-1} - q_{k+1} r_k \in (r_{k-1}, r_k) \subseteq (a,b)$

Ex in book: Showing things aren't Euclidean. (try it in $\mathbb{Z}$!).

Induction

$\cdots \Rightarrow r_n \in (a,b)$ ☆.

PIDs:

Def^n: A Principal ideal Domain (PID) is an int. domain where all ideals are principal.

Prop (before) ED $\Rightarrow$ PID.

Ex: $\mathbb{Z}, \mathbb{Z}[i]$ are PIDs.

- $\mathbb{Z}[x]$ is not even a PID, as $(2, x)$ isn't princ.
- (Book shows): $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ring of int in $\mathbb{Q}(\sqrt{-19})$ is a PID,

GCDs exist in PIDs, not always easy to compute not Euclidean

Prop: R a PID, $a, b \neq 0$ in R. Let d be gen. of (a,b).

1). $d = \gcd(a,b)$

2). d an R-lin. comb. of a, b

3). d unique up to mult. by a unit

(4) Pf follows this above.

null; In general, max^l ideal $\Rightarrow$ prime ideal.
saw converse held in $\mathbb{Z}$. (except for (0)).

Prop: In a PID, non-zero prime ideals are max^l.

Pf: Let (p) be a non-zero prime, $I=(m)$ any ideal $\supseteq (p)$.

Want: $I=(p)$ or R.

$p\in(m) \Rightarrow p=rm$, some $r\in R$.

(p) prime $\Rightarrow rm\in(p) \Rightarrow r\in(p)$ or $m\in(p)$.

If $m\in(p)$, then $(p)=(m)=I$.

If $r\in(p)$, say $r=ps \Rightarrow p=rm=psm$
$\Rightarrow sm=1$ (R is a domain)
$\Rightarrow m$ is a unit $\Rightarrow I=(m)=R$.

Cor: R comm. ring.
$R[x]$ PID (or ED) $\Rightarrow R$ a field. (saw converse before).

Pf: $R[x]$ PID. $R\leq R[x]$ is thus an integral domain.
($R[x]$ has $1 \Leftrightarrow R$ does).

Now (x) is a non-zero prime as $R[x]/(x)\cong R$
$\Rightarrow (x)$ is max^l $\Rightarrow R\cong R[x]/(x)$ is a field.

Ex: Division in $\mathbb{Z}[\sqrt{-2}]$,

Norm map: $N(x+y\sqrt{-2})=x^2+2y^2$. (recall: $N(\alpha\beta)=N(\alpha)N(\beta)$)

Given $a, b \in \mathbb{Z}[\sqrt{-2}]$, $b \neq 0$, $\exists\, q, r \in \mathbb{Z}[\sqrt{-2}]$

$a = qb + r$, $N(r) < N(b)$?

Claim: $\forall z \in \mathbb{Q}(\sqrt{-2})$, $\exists\, q \in \mathbb{Z}[\sqrt{-2}]$, $N(z-q) < 1$.

Given this, let $z = \frac{a}{b}$, choose q s.t. $N(\frac{a}{b} - q) < 1$

$\Rightarrow N(a - qb) < N(b)$, let $r = a - qb$ (just like in $\mathbb{Z}[i]$).

Pf of claim: write $z = x + y\sqrt{-2}$, $x, y \in \mathbb{Q}$.

Let m, n be the nearest ints to x, y (possibly non-unique).

So $|x-m| \leq \frac{1}{2}$, $|y-n| \leq \frac{1}{2}$.

Let $q = m + n\sqrt{-2}$.

$$\Rightarrow N(z-q) = N((x-m) + (y-n)\sqrt{-2})$$

$$= |x-m|^2 + 2|y-n|^2$$

$$\leq \frac{1}{4} + 2 \cdot \frac{1}{4} \leq \frac{3}{4} < 1$$ ∎

Works the same for $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-3}]$

as estimate becomes $N(z-q) = |x-m|^2 + |y-n|^2 d$

$\leq \frac{1}{4} + d \cdot \frac{1}{4}$ (fine up at -3).

fails for $\mathbb{Z}[\sqrt{-5}]$. We will see that is not a E.D.

Why? It is not a UFD:

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

primes.

If all things were UFDs, Diophantine stuff would be much easier.

$\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$

$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$ why? $\mathbb{Q}(\sqrt{-163})$ ... $\mathbb{Z}[\ldots]_{163}$ a UFD!