LECTURE 30. Dec. 1/2003.

§ Last time:

$R \hookrightarrow F =$ field of fractions of R.

$\uparrow$

R is an integral domain.

(which means: if $a \cdot b = 0$ in R then either $a=0$ or $b=0$ in R)

Examples of domains:

F field, $\mathbb{Z}$, $F[X]$ (F a field), or more generally $R[X]$ (R a domain)

Non-examples: $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$.

Then define "field of fractions":

$$F = \{a/b : a \in R, b \neq 0 \text{ in } R\}/\sim$$

$$a/b \sim a'/b' \iff ab' = a'b \quad \text{in } R$$

Then $R \hookrightarrow F$

$a \longmapsto a/1$ (which has inverse $1/a$)

---

§ Factorization in $\mathbb{Z}$:

0) Euclidean algorithm:

$$a, b \in \mathbb{Z} \Rightarrow b = ma + r, \quad 0 \leq r < |a|$$

1) Every ideal $I \neq (0)$ is principal, Specifically $I = (d)$ where d is smallest positive integer in I.

2) In particular, $I = (a, b) = (d)$
where $d = \gcd(a, b)$ ($\&$ $d = ma + nb$ by (*))

3) If p is a prime, and $p | ab$, then either $p | a$ or $p | b$

Pf) If $p \nmid a$ then $\gcd(a, p) = 1$
So $1 = ma + np \Rightarrow b = m(ab) + n(pb)$
so b is divisible by p. $\boxtimes$

4) Every integer n has a <u>unique</u> factorization into primes (up to reordering) $n = \pm p_1 \cdots p_k$.

Pf) (by induction on # of factors)

- If prime divides one factorization then it divides other, so use induction hypothesis $\Rightarrow$ unicity
- Existence follows because must have some prime divisor if >1 in abs. val. Then keep dividing out by primes — this must eventually stop because numbers are decreasing in abs. val. $\boxtimes$

Another ring R with a "Euclidean algorithm" is $R = F[X]$ (F a field):

0) $g(x) = f(x)\,q(X) + r(X)$ where $\deg(r(X)) < \deg(f(X))$

1) $I = (d(X))$ generated by $d(X)$ of least degree in I

2) Any two polys f and g have a gcd $(d) = (f, g) = I$

$d(X) = m(X)f(X) + n(X)g(X)$

3) We say $p(X)$ is a <u>prime poly</u> (<u>irred. or poly</u>) if any factorization $p(X) = p_1(X)\,p_2(X)$ has $\deg p_i = 0$ for $i = 1$ or 2.

So: if $p(X) \mid a(X)b(X)$, then $p(X) \mid a(X)$ or $p(X) \mid b(X)$

[by same argument as for $\mathbb{Z}$ — <u>see above</u>]

4) Any $f(X) = c \cdot p_1(X) \cdots p_k(X)$ <u>unique</u> factorization (up to reordering) into "primes" (<u>irreducible polynomials</u>).

<u>Def'n</u> Let R be an ~~integral~~ domain.

We say R is a <u>Euclidean domain</u>, if there is a fn $\delta : R \setminus \{0\} \to \{0, +1, +2, +3, \dots\}$ such that for any $a, b \in R$

$\exists\, q, r \in R$ s.t. $a = bq + r$ & either $r = 0$ & $\delta(r) < \delta(b)$

Gauss: The ring $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ is Euclidean, with size function: $\delta(a+bi) = a^2+b^2 = |a+bi|^2$

Cor: Every ideal $I \subset \mathbb{Z}[i]$ is principal, the ideal we constructed 2 weeks ago w/ $\mathbb{Z}[i]/I \simeq \mathbb{Z}/p\mathbb{Z}$ (where $p \equiv 1 \pmod 4$) is generated by a single element $a+bi$
$\Rightarrow a^2+b^2 = p$ (Fermat)

→ Refer to book for proof that $\mathbb{Z}[i]$ is Euclidean. (pp. 397-8)

Note: This proof doesn't work for, say $R = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{-5}]$
$\delta(a+b\sqrt{-5}) = a^2+5b^2$.
In fact R is not Euclidean (for any choice of δ) as the number 6 in R has 2 distinct factorizations $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ (& $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are distinct primes in R!) Moreover $I = (2, 1+\sqrt{-5})$ is not principal ($R/I \simeq \mathbb{Z}/2\mathbb{Z}$ $a+b\sqrt{-5} \mapsto a+b \bmod 2$)

We have shown:

R Euclidean

$\Downarrow$

R is a PID (Principal Ideal Domain)
(meaning: every ideal $I < R$ is of the form $I = (d)$ for some $d \in R$)

$\Downarrow$

R has unique factorization into prime elements

Rethink "divide", "prime" in terms of ideals:

- a divides b in R $\iff$ $b = ma$ $m \in R$ $\iff$ $b \in (a) \iff (b) \subset (a)$
- a divides b properly if neither a nor m is a unit in R $\iff$ $(b) \subsetneqq (a) \subsetneqq R$
  (m is not a unit) (a is not unit)
- p is prime, is irreducible, in R if p is not a unit & p has no proper factor in R $\iff$ $(p) \subsetneqq R$ is maximal among the principal ideals.

If R is a PID, then p is a prime $\iff$ (p) is a maximal ideal of R $\iff$ $R/(p)$ is a field.

In a general ideal $\subset$ ring situation: $R/(p)$ is an integral domain $\iff$ (p) is prime.

Example of a non-PID:

$R = \mathbb{Z}[X]$

$I = (X)$ $\qquad R/I \simeq \mathbb{Z}$ integral

$\qquad f(X) \mapsto f(0)$

So: X is prime in R.

But R/I is not a field, so R cannot be a PID. (by the above reasoning)

E.g.: $(X, 2)$ is a larger ideal (but still proper)

$(X, 2)$ is not principal.