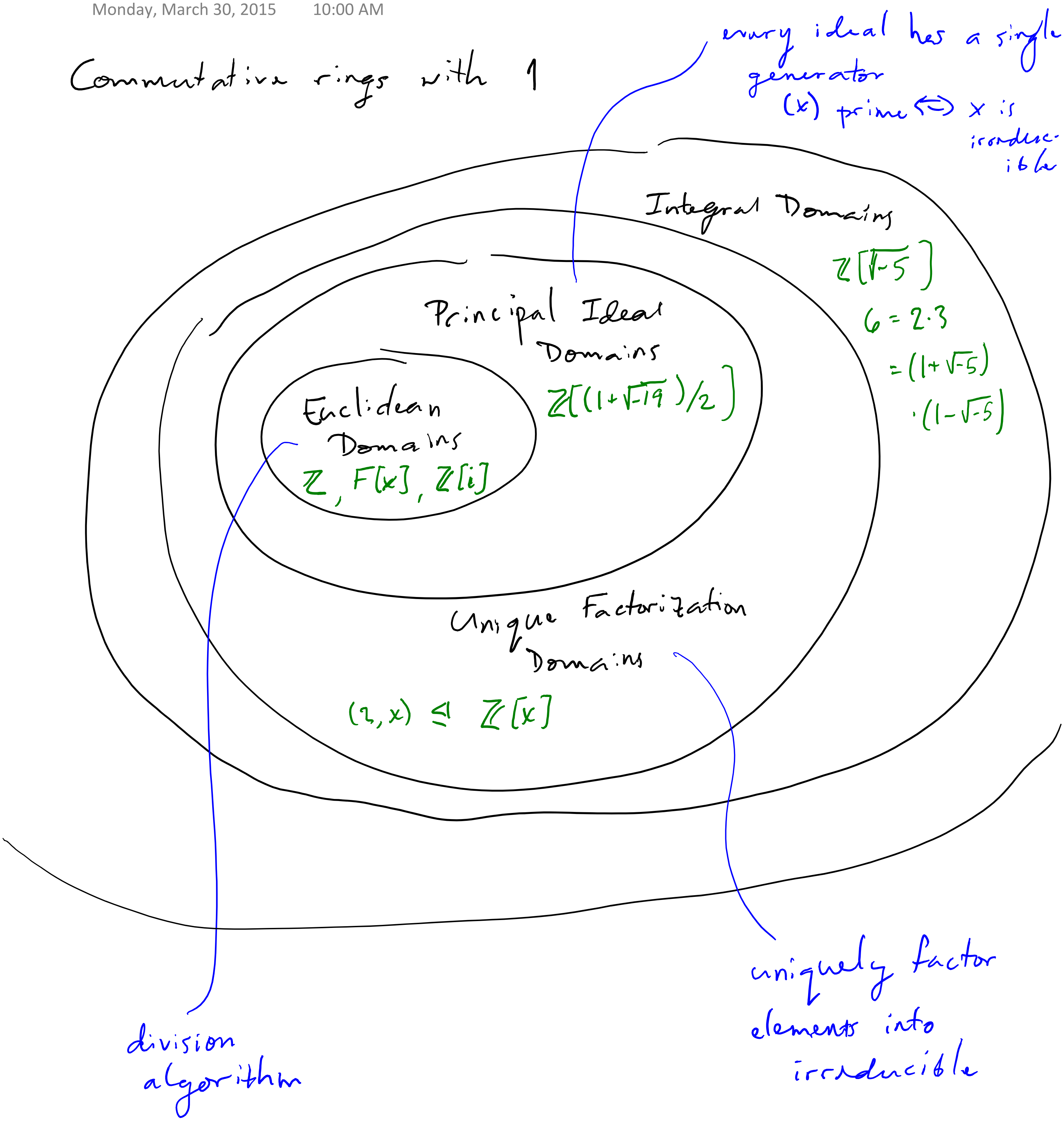
Lecture 32

Monday, March 30, 2015 10:00 AM

Commutative rings with 1



Euclidean Domains

R is an integral domain

Defn A function $N: R \longrightarrow \mathbb{N}$ w/ $N(0) = 0$ is a **norm** on R. If $N(a) > 0$ $\forall a \neq 0 \in R$, then N is a **positive norm**.

Defn R is a **Euclidean domain** if $\exists$ norm N on R s.t. $\forall a, b \in R$, $b \neq 0$ $\exists q, r \in R$ s.t.

$$a = \underset{\text{quotient}}{q}\, b + \underset{\text{remainder}}{r} \quad \text{and} \quad r = 0 \text{ or } N(r) < N(b)$$

division algorithm

When R admits a division algorithm, we get a Euclidean algorithm:

$$a = q_0 b + r_0 \qquad N(b) > N(r_0)$$

$$b = q_1 r_0 + r_1 \qquad N(r_0) > N(r_1)$$

$$r_0 = q_2 r_1 + r_2 \qquad N(r_1) > N(r_2)$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad N(r_n) > N(r_{n-1})$$

final stage at which the remainder is nonzero.

$$r_{n-1} = q_{n+1} r_n + 0$$

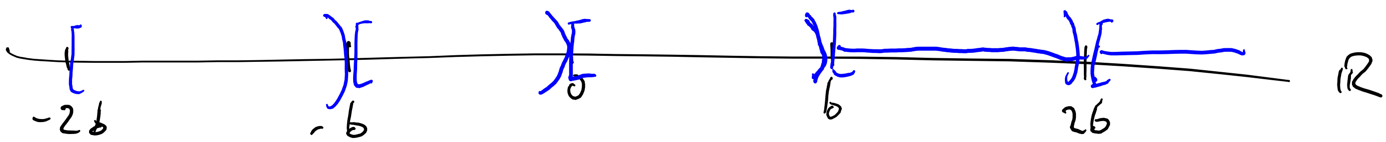
Terminates b/c $N(b) > N(r_0) > N(r_1) > \dots$ is a descending sequence of natural #s.

e.g. ⓪ Fields w/ any norm have a div alg:

$$q = ab^{-1}, \quad r = 0.$$

① $\mathbb{Z}$ w/ $N(a) = |a|$.

$a, b \in \mathbb{Z}, \quad b \neq 0$



$a \in [kb, (k+1)b), \quad k \in \mathbb{Z}.$

set $q = k$ to get $a - qb \in [0, |b|)$

Thus $a = qb + r$, where $|r| < |b|$.

② F a field, $F[x]$ w/ $N(p(x)) = \deg(p(x))$

admits a division algorithm.

③ The Gaussian integers $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$.

$N(a+bi) = a^2+b^2$.

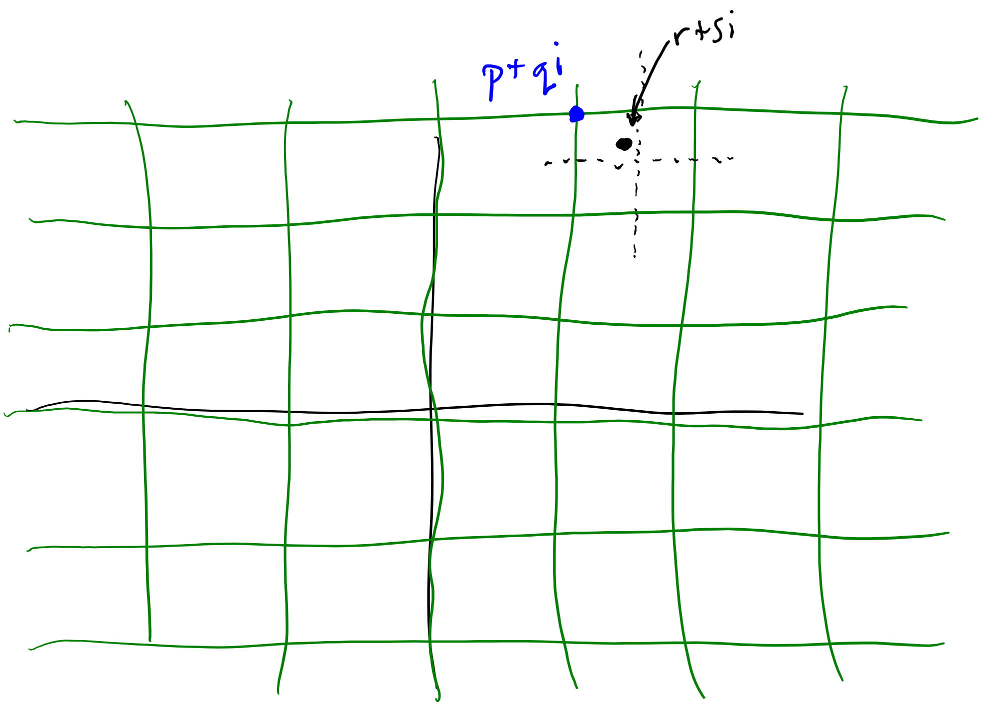
Set $\alpha = a+bi$, $\beta = c+di \neq 0$.

Then $\dfrac{\alpha}{\beta} = \dfrac{ac+bd}{c^2+d^2} + \dfrac{bc-ad}{c^2+d^2}\, i \in \mathbb{Q}(i)$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| $

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad \{e+fi \mid e,f \in \mathbb{Q}\}$

$= r + si$



Choose $p+qi \in \mathbb{Z}[i]$ s.t. $|r-p|, |s-q| \le \frac{1}{2}$

Claim $\gamma = \alpha - (p+qi)\beta \in \mathbb{Z}[i]$ w/ $N(\gamma) \le \frac{1}{2} N(\beta)$

But $\gamma = \left(\frac{\alpha}{\beta} - (p+qi)\right)\beta = ((r-p) + (s-q)i)\beta$

$$N((r-p)+(s-q)i) = (r-p)^2 + (s-q)^2$$
$$\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

and N is multiplicative so

$$N(\gamma) \leq \frac{1}{2} \cdot N(\beta). \qquad \square$$

④ Discrete valuation rings $\mathcal{O}_v \subseteq K$ via

$$N(x) = \begin{cases} v(x) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

If $v(a) < v(b)$ then $a = 0 \cdot b + a$

If $v(a) \geq v(b)$, then $q = ab^{-1} \in \mathcal{O}_v$ b/c

$$v(ab^{-1}) = v(a) - v(b) \geq 0$$

so $a = qb + 0$ works.

<u>Prop</u> Euclidean domains are PIDs.

<u>Pf</u> Suppose $I \trianglelefteq R$ in a ED R, $I \neq 0$. Take $0 \neq d \in I$ with $N(d)$ minimal in $N(I \setminus \{0\})$.

Have $(d) \subseteq I$. For $a \in I$, write

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

$N(r) < N(d)$ contradicts minimality of $N(d)$, so
$r = 0$ and $a = qd \implies a \in (d)$

Thus $I \subseteq (d) \implies I = (d)$.

<u>Cor</u> $\mathbb{Z}[x]$ is not a ED b/c it's not a PID.

<u>Fact</u> $\mathbb{Z}[\sqrt{-5}]$ is not a ED b/c $I = (3, 2+\sqrt{-5})$ is not principal.

Greatest common divisors:

R a comm ring w/ 1

<u>Definition</u> For $a, b \in R$, d is a <u>greatest common divisor</u> of a & b if

$(a, b) \subseteq (d)$ [d divides a & b]

and if $(a,b) \subseteq (d')$, then $(d) \subseteq (d')$

[any other divisor d' of a & b also divides d]

<u>Prop</u> If $(d) = (d') \trianglelefteq R$, then $d = ud'$ for $u \in R^\times$.

an integral domain

Pf WLOG, $d, d' \neq 0$.

Since $d \in (d')$, $\exists x$. $d = xd'$

$d' \in (d)$, $\exists y$. $d' = yd$

Thus $d = xyd \Rightarrow d(1-xy) = 0$

Since R is an integral domain & $d \neq 0$,

$1 - xy = 0 \Rightarrow 1 = xy \Rightarrow x, y \in R^\times$. $\square$