Lecture 28: Ring of Gaussian integers is Euclidean domain;

Tuesday, December 5, 2017 5:23 PM

<u>Proposition.</u> $\mathbb{Z}[i] := \{a+bi \mid a,b\in\mathbb{Z}\}$ is a Euclidean domain.

<u>Pf.</u> Let $N(a+bi) := a^2+b^2$. For $z_1 = a_1+ib_1$ and $z_2 = a_2+ib_2$ in $\mathbb{Z}[i]\setminus 0$, we have $\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{|z_2|^2} = \frac{a_1a_2-b_1b_2}{a^2+b^2} + i\,\frac{a_1b_2+a_2b_1}{a^2+b^2}$

$$\Rightarrow \frac{z_1}{z_2} = \underbrace{q_1+iq_2}_{\text{in } \mathbb{Z}[i]} + (\overline{r_1}+i\overline{r_2}) \quad \text{s.t. } \overline{r_1},\overline{r_2}\in\mathbb{Q}\cap(-1/2, 1/2].$$

$$\Rightarrow z_1 = (q_1+iq_2)\,z_2 + z_2(\overline{r_1}+i\overline{r_2})$$

Since $q := q_1+iq_2$, $z_1, z_2 \in \mathbb{Z}[i]$, we have

$$r := z_2(\overline{r_1}+i\overline{r_2}) = z_1 - qz_2 \in \mathbb{Z}[i].$$

And $|r|^2 = |z_2|^2(\overline{r_1}^2+\overline{r_2}^2) \le |z_2|^2\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{1}{2}|z_2|^2 < |z_2|^2$.

Hence $z_1 = qz_2 + r$ and $N(r) < N(q)$. ■

<u>Def.</u> Suppose D is an integral domain.

- $a\in D$ is called <u>irreducible</u> if $a\neq 0$, $a\notin D^\times$ and

$$a = xy \Rightarrow x\in D^\times \text{ or } y\in D^\times$$

- $a\in D$ is called <u>prime</u> if $a\neq 0$, $a\notin D^\times$ and

$$a\mid xy \Longrightarrow a\mid x \text{ or } a\mid y.$$

Lecture 28: Irreducible and prime elements

Friday, December 8, 2017 8:50 AM

- $a, b \in D$ are called <u>associates</u> if $\exists\, u \in D^\times$, $a = bu$.

<u>Lemma</u>. Suppose D is an integral domain, and $a \in D \setminus \{0\}$. Then

(1) a is prime $\iff \langle a \rangle$ is prime.

(2) a is irreducible $\iff \langle a \rangle$ is maximal among the proper principal ideals.

(3) b and c are associates $\iff \langle b \rangle = \langle c \rangle$.

<u>Pf</u>. (1) ($\Rightarrow$). a is prime $\Rightarrow a \notin D^\times \Rightarrow 1 \notin \langle a \rangle$

$\Rightarrow \langle a \rangle$ is proper.

- $bc \in \langle a \rangle \Rightarrow a \mid bc$

$\Rightarrow a \mid b$ or $a \mid c \Rightarrow b \in \langle a \rangle$ or $c \in \langle a \rangle$.

($\Leftarrow$). $\langle a \rangle$ is prime $\Rightarrow 1 \notin \langle a \rangle \Rightarrow a \in D^\times$.

- $a \mid bc \Rightarrow bc \in \langle a \rangle \Rightarrow b \in \langle a \rangle$ or $c \in \langle a \rangle$

$\Rightarrow a \mid b$ or $a \mid c$.

(2) ($\Rightarrow$). a is irred $\Rightarrow a \notin D^\times \Rightarrow 1 \notin \langle a \rangle \Rightarrow \langle a \rangle$ is proper.

- $\langle a \rangle \subsetneq \langle a' \rangle \Rightarrow a = a'b \Rightarrow$ either $a' \in D^\times$ or $b \in D^\times$.

<u>Case 1</u>. $b \in D^\times \Rightarrow a' = a b^{-1} \in \langle a \rangle \Rightarrow \langle a' \rangle \subseteq \langle a \rangle \subsetneq \langle a' \rangle$

which is a contradiction.

<u>Case 2</u>. $a' \in D^\times \Rightarrow \langle a' \rangle = D$; and the claim follows.

Lecture 28: Irreducible, prime, and being associate

Friday, December 8, 2017 11:01 AM

$(\Leftarrow)$. $\langle a\rangle$: proper $\Rightarrow a\notin D^\times$.

. $a=bc \Rightarrow a\in\langle b\rangle \Rightarrow \langle a\rangle\subseteq\langle b\rangle$

$\Rightarrow$ either $\langle a\rangle=\langle b\rangle$ or $\langle b\rangle = D$.

<u>Case 1</u>. $\langle b\rangle = D \Rightarrow 1\in\langle b\rangle \Rightarrow b\in D^\times$.

<u>Case 2</u>. $\langle a\rangle=\langle b\rangle \Rightarrow b=ac'$ for some $c'\in D$

$$\Rightarrow \left.\begin{matrix} a=bc=acc' \\ a\neq 0\end{matrix}\right\} \Rightarrow cc'=1 \Rightarrow c\in D^\times;$$

and the claim follows.

(3) $(\Rightarrow)$ $b=cu$ for some $u\in D^\times$

$$\Rightarrow \left.\begin{cases} b\in\langle c\rangle \Rightarrow \langle b\rangle\subseteq\langle c\rangle \\ c=bu^{-1} \Rightarrow c\in\langle b\rangle \Rightarrow \langle c\rangle\subseteq\langle b\rangle\end{cases}\right\} \Rightarrow \langle b\rangle=\langle c\rangle.$$

$$(\Leftarrow).\ \left.\begin{matrix}\langle b\rangle=\langle c\rangle \\ b=0\end{matrix}\right\} \Rightarrow c=0. \quad \text{Suppose } b\neq 0.$$

$$.\ \langle b\rangle=\langle c\rangle \Rightarrow \left.\begin{cases} b=cd \\ c=bd'\end{cases}\right\} \Rightarrow \left.\begin{matrix} b=bd'd \\ b\neq 0\end{matrix}\right\} \Rightarrow 1=d'd.$$

$$\Rightarrow \left.\begin{matrix} d\in D^\times \\ \text{and } b=cd\end{matrix}\right\} \Rightarrow b\sim c.$$

$\blacksquare$

<u>Lemma</u>. Suppose D is an integral domain, and $a\in D\setminus\{0\}$. Then

a is prime $\Rightarrow$ a is irreducible.

<u>Pf.</u> $a = bc \Rightarrow a \mid bc \Rightarrow a \mid b$ or $a \mid c$. W.L.O.G. we will assume $a \mid b$. So $\exists\, c' \in D$, $b = ac'$. Hence

$$\left.\begin{array}{l} a = bc = ac'c \\ a \neq 0 \end{array}\right\} \Rightarrow c'c = 1 \Rightarrow c \in D^{\times}. \qquad \blacksquare$$

<u>Cor.</u> Suppose D is a PID, and $a \in D \setminus \{0\}$. Then

$$a \text{ is prime} \iff a \text{ is irreducible}.$$

<u>Pf.</u> $(\Rightarrow)$ Previous lemma.

$(\Leftarrow)$ a is irred. $\Rightarrow$ $\left.\begin{array}{l}\langle a \rangle \text{ is max. among proper principal ideals} \\ D \text{ is a PID}\end{array}\right\}$

$\langle a \rangle$ is max. $\Rightarrow \langle a \rangle$ is prime

$\Rightarrow a$ is prime. $\blacksquare$

<u>Def.</u> Suppose D is an <u>integral domain</u>; we say D is a <u>Unique Factorization Domain</u> (UFD) if for any $a \in D \setminus (\{0\} \cup D^{\times})$

(1) $\exists\, p_i$'s irred. s.t. $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$.

(2) If $a = q_1 \cdots q_\ell$ for some irred. elements q_i, then $n = \ell$ and there is a permutation $\sigma \in S_n$ s.t. $\langle p_i \rangle = \langle q_{\sigma(i)} \rangle$ $(p_i \sim q_{\sigma(i)})$.

Lecture 28: PID implies UFD; the general idea of the existence part

Friday, December 8, 2017 11:28 AM

Ex.. Suppose F is a field.. Then we have seen that

$$F[x]^\times = F^\times = \{f(x) \in F[x] \mid \deg f = 0\}.$$

. If $\deg p = 1$, then $p(x)$ is irredu. in $F[x]$:

$$p(x) = f(x)\, g(x) \Rightarrow 1 = \deg f + \deg g$$

$$\Rightarrow \text{either } \deg f = 0 \text{ or } \deg g = 0$$

$$\Rightarrow \text{either } f \in F[x]^\times \text{ or } g \in F[x]^\times.$$

Notice that $2x$ is irred. in $\mathbb{Q}[x]$, but it is <u>reducible</u> in $\mathbb{Z}[x]$: $2x = (2)(x)$ and $2, x \notin \mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{\pm 1\}$.

(We will recall Gauss' lemma in Math 200 B; Gauss' lemma gives us the connection between irred. $/\mathbb{Z}$ and irred. $/\mathbb{Q}$.)

<u>Theorem</u>. If D is a PID, then D is a UFD.

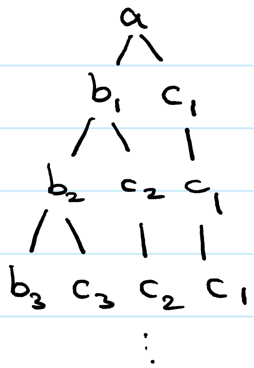
Idea of proof of existence.

$a \in D \setminus (\{0\} \cup D^\times)$. We'd like to write $\underline{a}$ as a prod. of irreducibles. If a is irreducible, we are done. If not, $a = b_1 c_1$; If both b_1 and c_1 are irred. we are done; if not,

Lecture 28: The existence part; and Noetherian rings

Friday, December 8, 2017 11:40 AM

we continue this process. So we get



$\langle a\rangle \subsetneq \langle b_1\rangle \subsetneq \langle b_2\rangle \subsetneq \cdots$

Is this possible?

For $\mathbb{Z}$, looking at the size of these numbers, we can deduce that this process terminates. For $F[x]$, we can use the deg. of poly. to show that this process terminates. How about in general?

<u>Def</u>. Suppose R is a unital ring. We say R is <u>Noetherian</u> if
any chain of ideals has a maximum.

<u>Lemma</u>. A unital ring R is Noetherian if and only if

$$\forall\, \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots,\ \mathfrak{a}_i \trianglelefteq R \text{ imply } \exists\, n_0,\ \mathfrak{a}_{n_0} = \mathfrak{a}_{n_0+1} = \cdots .$$

(This is called the ascending chain condition a.c.c.)

<u>Pf</u>. ($\Rightarrow$) Let $C := \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots\}$. Then C is a chain. So it has a maximum, say $\mathfrak{a}_{n_0}$. So $\forall\, i \geq n_0$, $\mathfrak{a}_i \subseteq \mathfrak{a}_{n_0} \subseteq \mathfrak{a}_i$

$$\Rightarrow \mathfrak{a}_i = \mathfrak{a}_{n_0}.$$

($\Leftarrow$) Suppose C is a chain of ideals with no maximum. We recursively define a sequ. $\{\mathfrak{a}_i\}_{i=1}^{\infty}$ of ideals.

Lecture 28: Noetherian condition

Friday, December 8, 2017 11:52 AM

$C \neq \emptyset \Rightarrow$ let $\mathfrak{a}_1 \in C$. Suppose we have already defined $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_n$; and $\mathfrak{a}_i \in C$. Since C does not have a maximum, $\exists\, \mathfrak{a}_{n+1} \in C$ s.t. $\mathfrak{a}_{n+1} \not\subseteq \mathfrak{a}_n$. As C is a chain, we have $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$. Hence we get a strictly ascending chain of ideals: $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots$ which is a contradiction. ∎

Theorem. Suppose R is a unital ring.

R is Noeth. $\iff$ any ideal is finitely generated.

Pf. ($\Rightarrow$) Let $\mathfrak{a}$ be an ideal. Suppose $\mathfrak{a}$ is not finitely generated. We recursively define a seq. $\{a_i\}_{i=1}^{n}$ s.t.

- $a_i \in \mathfrak{a}$ and $\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle \subsetneq \langle a_1, a_2, a_3\rangle \subsetneq \cdots$.

. Since $\mathfrak{a}$ is not f.g., $\mathfrak{a} \neq 0$. So $\exists\, a_1 \in \mathfrak{a} \setminus \{0\}$.

Suppose we have already defined $a_1, \ldots, a_n$ s.t.

$$\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle \subsetneq \cdots \subsetneq \langle a_1, \ldots, a_n\rangle .$$

Since $\mathfrak{a}$ is not f.g., $\exists\, a_{n+1} \in \mathfrak{a} \setminus \langle a_1, \ldots, a_n\rangle$. And so

Lecture 28: Noetherian and the existence part

Friday, December 8, 2017 12:07 PM

$\exists$, $\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle \subsetneq \cdots$ which contradicts the a.c.c.

($\Leftarrow$) Suppose C is a chain of ideals of R. Then we have seen that $\bigcup_{\mathfrak{a}\in C} \mathfrak{a}$ is an ideal of R. So it is f.g.

$\Rightarrow \bigcup_{\mathfrak{a}\in C} \mathfrak{a} = \langle x_1, \ldots, x_n\rangle$. $\Rightarrow \forall i, \exists \mathfrak{a}_i \in C$ s.t. $x_i \in \mathfrak{a}_i$.

Since C is a chain, we have $\mathfrak{a}_{i_1} \subseteq \mathfrak{a}_{i_2} \subseteq \cdots \subseteq \mathfrak{a}_{i_n}$.

$\Rightarrow x_1, \ldots, x_n \in \mathfrak{a}_{i_n} \Rightarrow \langle x_1, \ldots, x_n\rangle \subseteq \mathfrak{a}_{i_n}$

$\Rightarrow \bigcup_{\mathfrak{a}\in C} \mathfrak{a} \subseteq \mathfrak{a}_{i_n}$

$\Rightarrow \forall \mathfrak{a} \in C, \mathfrak{a} \subseteq \mathfrak{a}_{i_n} \Rightarrow \mathfrak{a}_{i_n}$ is the maximum of C. $\blacksquare$

<u>Cor.</u> A PID is Noetherian.

<u>Cor.</u> Any non-empty set Σ of ideals of a Noetherian ring has a <u>maximal</u> element. (<u>Exercise</u>. Use Zorn's lemma and Noeth. condition.)

<u>Pf of existence.</u> Let

$$\Sigma := \{\langle a\rangle \mid a \in D\setminus(\{0\}\cup D^\times),\ a \text{ cannot be written as a product of irreducibles}\}.$$

We'd like to show $\Sigma = \emptyset$. Suppose to the contrary that $\Sigma \neq \emptyset$.

Lecture 28: Existence part

Friday, December 8, 2017 12:20 PM

Then by the previous corollary, Σ has a maximal element $\langle a\rangle$. So a cannot be irreducible; that means $\exists\, b, c \notin D^\times$, $a = bc$. So $\langle b\rangle \supsetneq \langle a\rangle$ and $\langle c\rangle \supsetneq \langle a\rangle$. Since $\langle a\rangle$ is maximal in Σ, we deduce that $\langle b\rangle, \langle c\rangle \notin \Sigma$. So b and c can be written as products of irred; say,

$b = p_1 \cdots p_n$ and $c = p_{n+1} \cdots p_{n+m}$ where p_i's are irred.

Then $a = bc = p_1 \cdots p_n p_{n+1} \cdots p_{n+m}$ can be written as a product of irredu. which is a contradiction.

<u>Pf of uniqueness.</u>

Suppose $p_1 \cdots p_n = q_1 \cdots q_m$ and p_i's and q_j's are irreducible.

Then p_i's and q_j's are prime. So

$$q_1 \mid p_1 \cdots p_n \Rightarrow q_1 \mid p_1 \text{ or } q_1 \mid p_2 \cdots p_n$$

$$\Rightarrow \text{(inductively) } \exists\, i,\ q_1 \mid p_i.$$

$$\Rightarrow \underbrace{\langle p_i\rangle}_{\text{max.}} \subseteq \langle q_1\rangle \subsetneq D \Rightarrow \langle p_i\rangle = \langle q_1\rangle \Rightarrow p_i \sim q_1.$$

We write $p_i = u_i q_1$ and cancel q_1; and continu. recursively. ■