Lecture 12: A Euclidean domain is a PID

Monday, April 30, 2018 11:12 AM

<u>Recall</u>. An integral domain D is called a Euclidean domain if

$\exists N: D \to \mathbb{Z}^{\geq 0}$, (1) $N(d)=0 \Leftrightarrow d=0$

(2) $\forall a \in D, b \in D\setminus\{0\}, \exists q, r \in D,$

$\cdot\ a = bq + r$

$\cdot\ N(r) < N(b)$

We proved $\mathbb{Z}[i]$ and $F[x]$, where F is a field, are EDs.

<u>Theorem</u>. A Euclidean domain is a PID.

<u>Pf</u>. Suppose $I \trianglelefteq D$. If $I=0$, then it is principal. So assume $I \neq 0$.

Consider $\{N(a) \mid a \in I, a \neq 0\}$. Since it is a non-empty subset of $\mathbb{Z}^+$, it has a minimum. Suppose $a_0 \in I$ is s.t.

$$N(a_0) = \min\{N(a) \mid a \in I, a \neq 0\}.$$

<u>Claim</u>. $I = \langle a_0 \rangle$.

<u>Pf</u>.. Since $a_0 \in I$, $\langle a_0 \rangle \subseteq I$.

. For $a \in I$, $\exists q, r \in D$ s.t. $a = a_0 q + r$ and $N(r) < N(a_0)$

$$\left.\begin{array}{l} \Rightarrow\ r = a - a_0 q \in I \ \text{ and } \ N(r) < N(a_0) \\ \text{Since } N(a_0) = \min\{N(a) \mid a \in I, a \neq 0\} \end{array}\right\} \Rightarrow r = 0 \Rightarrow a \in \langle a_0 \rangle.$$

■

Lecture 12: Certain factors of Gaussian integers

Monday, April 30, 2018 11:12 AM

<u>Corollary</u>. Suppose $a^2+b^2=p$ is prime in $\mathbb{Z}$ and $a,b\in\mathbb{Z}$. Then

$$\mathbb{Z}[i]/\langle a+bi\rangle \simeq \mathbb{Z}/p\mathbb{Z}.$$

<u>Pf</u>. <u>Step 1.</u> $p\nmid a$ and $p\nmid b$.

<u>Pf</u>. Suppose to the contrary $p\mid a$. Then either $p=0$ or $p\le |a|$.

- If $p=0$, then $b^2=p$ which is a contradiction as p is prime
- If $p\le |a|$, then $p^2\le a^2\le a^2+b^2=p$ which is again a contradi. as $p>1$.

<u>Step 2.</u> $\exists\, \alpha\in\mathbb{Z}$ s.t. $\alpha^2\equiv -1 \pmod p$ and $a+\alpha b\equiv 0 \pmod p$ $(*)$

<u>Pf</u> $a^2+b^2=p$ implies $\bar{a}^2+\bar{b}^2=\bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$

since $p\nmid b$, $\bar{b}\neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, $(\bar{a}/\bar{b})^2=-1$. So $\alpha+p\mathbb{Z} = -\bar{a}/\bar{b}$ satisfies $(*)$.

<u>Step 3.</u> $\phi:\mathbb{Z}[i]\to\mathbb{Z}/p\mathbb{Z}$, $\phi(c+id)=c+\alpha d+p\mathbb{Z}$ a ring homomorphism.

Lecture 12: Certain factors of Gaussian integers

Monday, April 30, 2018 11:31 AM

(addition: exercise)

$$\phi((c_1+id_1)(c_2+id_2)) = \phi((c_1c_2-d_1d_2)+i(c_1d_2+c_2d_1))$$
$$= (c_1c_2-d_1d_2)+\alpha(c_1d_2+c_2d_1)+p\mathbb{Z}.$$

$$\phi(c_1+id_1)\,\phi(c_2+id_2) = (c_1+\alpha d_1+p\mathbb{Z})(c_2+\alpha d_2+p\mathbb{Z})$$
$$= (c_1c_2+\alpha^2 d_1d_2+\alpha(c_1d_2+d_1c_2))+p\mathbb{Z}$$

$\boxed{\alpha^2 \equiv -1 \pmod p}$

$$= (c_1c_2-d_1d_2)+\alpha(c_1d_2+d_1c_2)+p\mathbb{Z}$$

and claim follows.

Step 4. ϕ is onto.

$\forall \bar{a} \in \mathbb{Z}/p\mathbb{Z}$, $\quad \bar{a} = a+p\mathbb{Z} = \phi(a)$.

Step 5 $\quad a+bi \in \ker \phi$.

Pf $\quad \phi(a+bi) = a+b\alpha+p\mathbb{Z} = \bar{0}$. (by step 2).

Step 6. $\ker\phi = \langle a+bi \rangle$.

Pf Since $\mathbb{Z}[i]$ is a E.D., it is a PID. So

$\ker\phi = \langle a'+b'i \rangle$. Since $\langle a+bi \rangle \subseteq \ker\phi$,

$a+bi = (a'+b'i)(c+di)$ for some $c, d \in \mathbb{Z}$. Hence

Lecture 12: Certain factors of Gaussian integers

Monday, April 30, 2018   11:44 AM

$\Rightarrow a^2+b^2 = (a'^2+b'^2)(c^2+d^2) \Rightarrow (a'^2+b'^2)(c^2+d^2) = p.$

Since p is prime, either $a'^2+b'^2=p$ and $c^2+d^2=1$ or $a'^2+b'^2=1$ and $c^2+d^2=p$.

Claim. $a'^2+b'^2 \neq 1$.

Pf. If $a'^2+b'^2=1$, then $1=(a'+ib')(a'-ib') \in \ker\phi$; this contradicts $\phi(1) = 1+p\mathbb{Z} \neq 0+p\mathbb{Z}$. $\square$

By the above claim, $c^2+d^2=1$. Hence $(c+id)(c-id)=1$, which implies $c+id \in U(\mathbb{Z}[i])$. Therefore

$$\langle a+bi\rangle = \langle (a'+b'i)(c+id)\rangle \underset{\boxed{c+id\,\in\, U(\mathbb{Z}[i])}}{=} \langle a'+b'i\rangle.$$

Thus $\ker\phi = \langle a+bi\rangle$. And so by the 1st isomorphism theorem $\mathbb{Z}[i]/\langle a+bi\rangle = \mathbb{Z}[i]/\ker\phi \simeq \operatorname{Im}\phi = \mathbb{Z}/p\mathbb{Z}$. $\blacksquare$

As we mentioned earlier, ideals were defined to extend our number theoretic techniques to rings other than $\mathbb{Z}$.

Lecture 12: Prime ideals

Monday, April 30, 2018 11:14 AM

We start with defining prime ideals;

Def. Suppose R is a unital commutative ring. An ideal I of R is called a prime ideal if $I \neq R$ and

$$ab \in I \Rightarrow \text{either } a \in I \text{ or } b \in I.$$

Ex. What are prime ideals of $\mathbb{Z}$?

Solution. As $\mathbb{Z}$ is a PID, any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}^{\geq 0}$.

- If n is composite, then $\exists\, a, b \in \mathbb{Z}$ s.t. $1 < a, b < n$, $n = ab$. Hence $ab = n \in n\mathbb{Z}$, and $a \notin n\mathbb{Z}$, $b \notin n\mathbb{Z}$. And so $n\mathbb{Z}$ is not a prime ideal.
- If $n = 1$, then $n\mathbb{Z} = \mathbb{Z}$ is not a proper ideal; and so it is not a prime ideal.
- If $n = 0$, then $n\mathbb{Z} = \{0\} \underset{\neq}{\trianglelefteq} \mathbb{Z}$, and

$$ab \in \{0\} \Rightarrow ab = 0 \underset{\boxed{\mathbb{Z} \text{ is integral domain}}}{\Rightarrow} a = 0 \text{ or } b = 0 \Rightarrow a \in \{0\} \text{ or } b \in \{0\}.$$

Lecture 12: Prime ideals

Monday, April 30, 2018 2:42 PM

and so $\{0\}$ is a prime ideal.

- If $n=p$ is prime, then $p\mathbb{Z}$ is a proper ideal and

$ab\in p\mathbb{Z} \Rightarrow p\mid ab \underset{\boxed{\text{Euclid's lemma}}}{\Rightarrow} p\mid a$ or $p\mid b \Rightarrow a\in p\mathbb{Z}$ or $b\in p\mathbb{Z}$.

And $p\mathbb{Z}$ is a prime ideal.

Hence an ideal I of $\mathbb{Z}$ is prime if and only if $I=\{0\}$ or $I=p\mathbb{Z}$ for some prime p.

<u>Remark</u>. The Euclid's lemma was the main source of the given definition of prime ideals.

In the next lecture we will prove:

<u>Proposition</u>. Suppose R is a unital commutative ring and $I \trianglelefteq R$. Then I is a prime ideal $\Leftrightarrow$ R/I is an integral domain.