Lecture 11: A factor ring of Gaussian integers

Friday, April 27, 2018 10:59 AM

We were proving $\mathbb{Z}[i]/\langle 3+2i\rangle \simeq \mathbb{Z}/13\mathbb{Z}$; we defined

$\theta: \mathbb{Z}[i] \longrightarrow \mathbb{Z}/13\mathbb{Z}$, $\theta(a+bi) = a+5b+13\mathbb{Z}$ and proved

θ is an onto ring homomorphism and $3+2i \in \ker\theta$.

Suppose $a+bi \in \ker\theta$. Since $\mathbb{Q}[i]$ is a field, $\exists\, a', b' \in \mathbb{Q}$

s.t. $\dfrac{a+bi}{3+2i} = a'+b'i = q_1+q_2 i + e_1 + e_2 i$ for some

$q_1, q_2 \in \mathbb{Z}$ and $-\frac{1}{2} \le e_1, e_2 \le \frac{1}{2}$. Hence

$$\underbrace{a+bi}_{\text{in } \mathbb{Z}[i]} = \underbrace{(3+2i)(q_1+q_2 i)}_{\text{in } \mathbb{Z}[i]} + \underbrace{(3+2i)(e_1+e_2 i)}_{r}$$

$$\Rightarrow r \in \mathbb{Z}[i] \text{ and } |r|^2 = |3+2i|^2 |e_1+e_2 i|^2 \le 13 \times (\tfrac{1}{4}+\tfrac{1}{4}) = 6.5.$$

As $3+2i$, $a+bi \in \ker\theta$, $r = r_1 + r_2 i \in \ker\theta$; and

$r_1^2 + r_2^2 \le 6.5$. And so $|r_i| \le 2$. Therefore

$$\left.\begin{array}{l} 13 \mid r_1 + 5r_2 \\ |r_i| \le 2 \Rightarrow |r_1+5r_2| \le 12 \end{array}\right\} \Rightarrow r_1 + 5r_2 = 0 \quad \circledast$$

$$\Rightarrow \left.\begin{array}{l} 5 \mid r_1 \\ |r_1| \le 2 \end{array}\right\} \Rightarrow r_1 = 0$$

And so by $\circledast$ $r_2 = 0$.

Therefore $a+bi = (3+2i)(q_1+q_2 i) \in \langle 3+2i\rangle$. ∎

Lecture 11: Euclidean domains

Friday, April 27, 2018 11:16 AM

In the examples that we have seen about $\mathbb{Z}$, $\mathbb{Q}[x]$, and $\mathbb{Z}[i]$ we saw the importance of having a generalized division algorithm. So we make it more concrete now:

<u>Def.</u> An integral domain D is called a Euclidean Domain (ED) if $\exists\, N: D \to \mathbb{Z}^{\geq 0}$ s.t. • $N(d)=0 \Leftrightarrow d=0$

• $\forall\, a\in D,\ b\in D\setminus\{0\},\ \exists\, q, r\in D$ s.t.

$$a = bq + r \quad \text{and} \quad N(r) < N(b). \qquad (*)$$

<u>Proposition.</u> $\mathbb{Z}$ is a Euclidean Domain.

<u>Pf.</u> Let $N: \mathbb{Z} \to \mathbb{Z}^{\geq 0}$, $N(a) = |a|$. Then $N(d)=0 \Leftrightarrow d=0$.

$\forall\, a\in\mathbb{Z},\ b\in\mathbb{Z}\setminus\{0\}$, by the division algorithm $\exists\, q, r\in\mathbb{Z}$ s.t.

(1) $a = bq + r$ and (2) $0 \leq r < |b|$. Hence

$N(r) = |r| = r < |b| = N(b)$; and so $\mathbb{Z}$ is a E.D. ∎

<u>Proposition.</u> Suppose F is a field. Then the ring of polynomials $F[x]$ with coefficients in F is a Euclidean domain.

Lecture 11: F[x] is a ED

Friday, April 27, 2018 1:51 PM

Pf. • $\deg(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = n$ if $a_n \neq 0$

• $\deg(0) = -\infty$.

Let $N: F[x] \to \mathbb{Z}^{\geq 0}$, $N(p(x)) = 2^{\deg p}$ with the convention that $2^{-\infty} = 0$. So $N(p(x)) = 0 \iff p(x) = 0$.

For any $a(x) \in F[x]$ and $b(x) \in F[x] \setminus \{0\}$, by strong induction on $\deg(a)$ we prove the existence of $q(x)$ and $r(x)$.

Before we start proof of strong induction, let's consider the following two cases:

• If $a(x) = 0$, then $q(x) = 0 = r(x)$ satisfy $(*)$

(I) • If $\deg a < \deg b$, then $q(x) = 0$ and $r(x) = a(x)$ satisfy $(*)$.

<u>Base of induction for $a \neq 0$.</u>

$\deg a = 0$; if $\deg b > 0$, we are done by (I).

If $\deg b = 0$, then $b \in F \setminus \{0\}$; and so $q = \frac{a}{b}$, $r = 0$ satisfy $(*)$.

Lecture 11: F[x] is a ED.

Friday, April 27, 2018 11:27 AM

- Strong induction step.

Suppose $a(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$, $c_n \neq 0$, and $b(x) = d_m x^m + d_{m-1} x^{m-1} + \cdots + d_0$, $d_m \neq 0$. If $n < m$, then $q(x) = 0$ and $r(x) = a(x)$ satisfy $(*)$.

If $n \geq m$, then $a(x) - \frac{c_n}{d_m} x^{n-m} b(x)$

(getting rid of the leading term $c_n x^n$.)

$$= (c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0)$$
$$- (c_n x^n + \frac{c_n}{d_m} \cdot d_{m-1} x^{n-1} + \cdots + \frac{c_n}{d_m} d_0 x^{n-m})$$
$$= \left(c_{n-1} - \frac{c_n d_{m-1}}{d_m}\right) x^{n-1} + \text{lower deg. terms}$$

$$\Rightarrow \deg\left(a(x) - \frac{c_n}{d_m} x^{n-m} b(x)\right) < \deg a(x)$$

By the strong induction hypothesis, $\exists\, q', r \in F[x]$ s.t.

$a(x) - \frac{c_n}{d_m} x^{n-m} b(x) = q'(x) \cdot b(x) + r(x)$ and $N(r) < N(b)$.

And so $a(x) = \underbrace{\left(\frac{c_n}{d_m} x^{n-m} + q'(x)\right)}_{q(x)} \cdot b(x) + r(x)$ and $N(r) < N(b)$. ∎

Lecture 11: The ring of Gaussian integers is a ED

Friday, April 27, 2018 11:37 AM

<u>Proposition</u> $\mathbb{Z}[i]$ is a ED.

<u>Pf.</u> Let $N: \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0}$, $N(a+bi) = a^2+b^2$.

For $a+bi \in \mathbb{Z}[i]$ and $c+di \in \mathbb{Z}[i]\setminus\{0\}$, since $\mathbb{Q}[i]$ is a field,

$\exists\, a', b' \in \mathbb{Q}$ s.t. $\dfrac{a+bi}{c+di} = a'+b'i$. So $\exists\, q, q' \in \mathbb{Z}$ and

$e, e' \in \mathbb{Q}$ s.t. $a' = q+e$, $b' = q'+e'$, $|e|, |e'| \leq 1/2$.

And so $a+bi = (q+q'i)(c+di) + \underbrace{(e+e'i)(c+di)}_{r}$

Since $a+bi$, $q+q'i$, and $c+di \in \mathbb{Z}[i]$, $r \in \mathbb{Z}[i]$.

And $N(r) = |(e+e'i)(c+di)|^2 = |e+e'i|^2\,|c+di|^2$

$$= (e^2+e'^2)(c^2+d^2) \leq \left(\tfrac{1}{4}+\tfrac{1}{4}\right)N(c+di) \leq \tfrac{1}{2}N(c+di).$$

Since $c+di \neq 0$, $N(c+di) \neq 0$ and $\frac{1}{2}N(c+di) < N(c+di)$; and

so $N(r) < N(c+di)$. ■

In the next lecture we will prove

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

We will consider the "smallest" element of I and show I is generated by that element.