Lecture 27: Finding primes

Monday, December 4, 2017 10:46 AM

Theorem. $\forall\ \mathfrak{a} \lhd A$, $S \subseteq A$ multiplicatively closed

Suppose $\mathfrak{a} \cap S = \emptyset$, and let

$$\sum_{\mathfrak{a},S} := \{\mathfrak{b} \lhd A \mid ① \ \mathfrak{a} \subseteq \mathfrak{b} \quad ② \ \mathfrak{b} \cap S = \emptyset\}.$$

Then (1) $\sum_{\mathfrak{a},S}$ has a maximal element w.r.t. $\subseteq$.

(2) A maximal element $\mathfrak{p}$ of $\sum_{\mathfrak{a},S}$ is a prime ideal

Pf. of theorem. (1) By Zorn's lemma, it is enough to show that any chain C of $\sum_{\mathfrak{a},S}$ has an upper-bound in $\sum_{\mathfrak{a},S}$.

Let $\tilde{\mathfrak{b}} := \bigcup_{\mathfrak{b} \in C} \mathfrak{b}$.

Since $C \subseteq \sum_{\mathfrak{a},S}$, $\forall\ \mathfrak{b} \in C$, $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{b} \cap S = \emptyset$.

And so $\mathfrak{a} \subseteq \bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ and $\left(\bigcup_{\mathfrak{b} \in C} \mathfrak{b}\right) \cap S = \emptyset$. So if we show $\bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ is an ideal, we deduce that $\bigcup_{\mathfrak{b} \in C} \mathfrak{b} \in \sum_{\mathfrak{a},S}$; and so $\bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ is an upper-bound of C in $\sum_{\mathfrak{a},S}$.

Claim. Since C is a chain, $\bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ is an ideal.

- $\forall\ a_1, a_2 \in \bigcup_{\mathfrak{b} \in C} \mathfrak{b}$, $\exists\ \mathfrak{b}_1, \mathfrak{b}_2 \in C$ s.t. $a_i \in \mathfrak{b}_i$.

Either $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ or $\mathfrak{b}_2 \subseteq \mathfrak{b}_1$ (C is a chain); and so

either $a_1, a_2 \in \mathfrak{b}_2$ or $a_1, a_2 \in \mathfrak{b}_1$. Hence either

$a_1 + a_2 \in \mathfrak{b}_2$ or $a_1 + a_2 \in \mathfrak{b}_1$. In either case

$$a_1 + a_2 \in \bigcup_{\mathfrak{b} \in C} \mathfrak{b}. \qquad (I)$$

$\forall\, a \in \bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ and $r \in A$, $\exists\, \mathfrak{b} \in C$ s.t. $a \in \mathfrak{b}$

$\Rightarrow ra \in \mathfrak{b} \Rightarrow ra \in \bigcup_{\mathfrak{b} \in C} \mathfrak{b}$. (II)

(I), (II) imply that $\bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ is an ideal; and the claim follows.

(2) Suppose $\mathfrak{p}$ is a maximal element of $\sum_{\mathfrak{a},S}$. Suppose $\exists\, a, b \in A$ s.t. $a, b \notin \mathfrak{p}$ and $ab \in \mathfrak{p}$. So $\langle a \rangle + \mathfrak{p}, \langle b \rangle + \mathfrak{p} \notin \sum_{\mathfrak{a},S}$. As $\mathfrak{a} \subseteq \langle a \rangle + \mathfrak{p}$ and $\mathfrak{a} \subseteq \langle b \rangle + \mathfrak{p}$, we deduce $\exists\, s_1 \in \langle a \rangle + \mathfrak{p} \cap S$ and $s_2 \in \langle b \rangle + \mathfrak{p}$. So $\exists\, r_1, r_2 \in A$ and $x_1, x_2 \in \mathfrak{p}$ s.t.

$$s_1 = r_1 a + x_1 \quad \text{and} \quad s_2 = r_2 b + x_2.$$

$$\Rightarrow s_1 s_2 = \underbrace{r_1 r_2 ab}_{\text{in } \mathfrak{p}} + \underbrace{r_1 a x_2}_{\text{in } \mathfrak{p}} + \underbrace{r_2 b x_1}_{\text{in } \mathfrak{p}} + \underbrace{x_1 x_2}_{\text{in } \mathfrak{p}} \in S$$

$\Rightarrow \mathfrak{p} \cap S \neq \emptyset$, which contradicts $\mathfrak{p} \in \sum_{\mathfrak{a},S}$. ∎

Lecture 27: Nilradical and primes

Tuesday, December 5, 2017 4:39 PM

Def. An element a of A is called **nilpotent** if $a^k = 0$ for some $k \in \mathbb{Z}^+$.

- $\mathrm{Nil}(A) := \{a \in A \mid a : \text{nilpotent}\}$.

Theorem. (1) $\mathrm{Nil}(A) \lhd A$.

(2) $\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$ where $\mathrm{Spec}(A)$ is the set of prime ideals of A.

Pf. (1). $a_1, a_2 \in \mathrm{Nil}(A) \Rightarrow \exists\, n_1, n_2 \in \mathbb{Z}^+,\ a_1^{n_1} = a_2^{n_2} = 0$.

$$(a_1 + a_2)^{n_1+n_2} = \sum_{\substack{i_1+i_2 = n_1+n_2 \\ 0 \le i_1, i_2}} \binom{n_1+n_2}{i_1} a_1^{i_1} a_2^{i_2}.$$

As $i_1 + i_2 = n_1 + n_2$, either $i_1 \ge n_1$ or $i_2 \ge n_2$. Hence either $a_1^{i_1} = 0$ or $a_2^{i_2} = 0$. Therefore in either case $a_1^{i_1} a_2^{i_2} = 0$.

Thus $(a_1 + a_2)^{n_1+n_2} = 0$, which implies $a_1 + a_2 \in \mathrm{Nil}(A)$.

- $a \in \mathrm{Nil}(A),\ r \in A \Rightarrow \exists\, n \in \mathbb{Z}^+,\ a^n = 0$

$$\Rightarrow (ra)^n = r^n a^n = 0 \Rightarrow ra \in \mathrm{Nil}(A).$$

(2) $a \in \mathrm{Nil}(A) \Rightarrow \exists\, n \in \mathbb{Z}^+,\ a^n = 0 \in \mathfrak{p} \Rightarrow a \cdot a^{n-1} \in \mathfrak{p}$
$\mathfrak{p} \in \mathrm{Spec}(A)$

Hence either $a \in \mathfrak{p}$ or $a^{n-1} \in \mathfrak{p}$. So inductively

we can show $a \in \mathfrak{p}$. So $\mathrm{Nil}(A) \subseteq \mathfrak{p}$, which implies

$$\mathrm{Nil}(A) \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}. \qquad (I)$$

Suppose $f \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \setminus \mathrm{Nil}(A)$. Then $S_f := \{1, f, f^2, \cdots\}$ does not contain zero; that means $S_f \cap \{0\} = \emptyset$. By theorem there is $\mathfrak{p}_0 \in \mathrm{Spec}(A)$ s.t. $\mathfrak{p}_0 \cap S_f = \emptyset$; this implies $f \notin \mathfrak{p}_0$, which contradicts $f \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$. Therefore

$$\bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \subseteq \mathrm{Nil}(A). \qquad (II)$$

(I), (II) imply $\bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathrm{Nil}(A)$. ∎

Exercise. Show that $\mathrm{Nil}(R[x]) = \mathrm{Nil}(R)[x]$.

We will come back to this type of result in math 200c. For now we'd like to find a technique to prove certain rings are unique factorization domains (UFD). You have seen the fundamental theorem of arithmetic which asserts that $\mathbb{Z}$ is a UFD. And its proof is based on division algorithm. Next we will make that argument as general as possible.

Lecture 27: Euclidean domains

Tuesday, December 5, 2017 5:07 PM

Def. An integral domain D is called a **Euclidean domain** if

$\exists\, N: D \to \mathbb{Z}^{\geq 0}$ s.t. (1) $N(d) \geq 0$ and

$N(d)=0 \iff d=0$.

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

$a = bq + r$ and

$N(r) < N(b)$.

(q is called a quotient of a divided by b, and

r is called a remainder of a divided by b.)

- Because of the division algorithm $\mathbb{Z}$ is a Euclidean Domain.

(Here $N: \mathbb{Z} \to \mathbb{Z}^{\geq 0}$, $N(a) := |a|$.)

- Because of the long division in $F[x]$ where F is a field, $F[x]$ is a Euclidean Domain.

(Here $N: F[x] \to \mathbb{Z}^{\geq 0}$, $N(f(x)) := 2^{\deg f}$; with the convention $2^{-\infty} = 0$.)

In the next lecture we will prove that the ring of Gaussian integers $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.

Lecture 27: A Euclidean domain is a PID

Wednesday, December 6, 2017 10:02 AM

Def. An integral domain D is called a Principal Ideal Domain (PID) if any ideal is principal.

Theorem. Any Euclidean Domain is a PID.

Pf. Suppose $\mathcal{A}$ is a non-zero ideal of D; and for $a_0 \in \mathcal{A}$

$$N(a_0) = \min \{ N(a) \mid a \in \mathcal{A} \setminus 0 \}.$$

Claim. $\mathcal{A} = \langle a_0 \rangle$.

Pf of claim. Clearly $\langle a_0 \rangle \subseteq \mathcal{A}$. Suppose $a \in \mathcal{A}$. Then

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

$\Rightarrow r = a - a_0 q \in \mathcal{A}$ (*)

Since $N(r) < N(a_0)$ and $N(a_0) = \min \{ N(b) \mid b \in D \setminus 0 \}$,

by (*) we deduce $r = 0$; this implies $a = a_0 q \in \langle a_0 \rangle$.

Hence $\mathcal{A} = \langle a_0 \rangle$. ∎

Corollary. $\mathbb{Z}$, $F[x]$ where F is a field, $\mathbb{Z}[i]$ are PID.

You will show that $\mathbb{Z}[x]$ is NOT a PID. We will prove that a PID is a UFD.