Lecture 02: Eisenstein's criterion

Friday, January 11, 2019 5:38 PM

One of the useful irreducibility criteria is due to Eisenstein:

__Theorem__. Suppose D is an integral domain, $\mathfrak{p} \in \mathrm{Spec}(D)$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in D[x]$. Suppose $a_n \notin \mathfrak{p}$, $a_0, \ldots, a_{n-1} \in \mathfrak{p}$, $a_0 \notin \mathfrak{p}^2$, and $\langle a_0, \ldots, a_n \rangle = D$. Then $f(x)$ is irreducible in $D[x]$.

__Remark__. In lecture we proved this only for monic polynomials for which automatically $\langle a_0, \ldots, a_n \rangle = D$.

- When D is a UFD, the condition $\langle a_0, \ldots, a_n \rangle = D$ implies that f is primitive; and this condition can be replaced with saying that f is primitive.
- The right condition instead of $\langle a_0, \ldots, a_n \rangle = D$ is saying that $(d \mid a_0, \ldots, d \mid a_n \Rightarrow d \in D^\times)$.

__Pf.__ Suppose to the contrary that $f(x) = g(x)\, h(x)$. If deg. of g or h is 1, then g or h divides all the coeff. of f. Since $\langle a_0, \ldots, a_n \rangle = D$, we deduce that either g or h is in $D^\times$.

Lecture 02: Eisenstein's criterion

Friday, January 11, 2019 11:57 PM

Next we assume $\deg g, \deg h \geq 1$. So

$$g(x)\, h(x) = f(x) \equiv a_n x^n \pmod{\mathfrak{p}}. \quad (1)$$

<u>Claim.</u> $g(0), h(0) \in \mathfrak{p}$.

<u>Pf of Claim.</u> Suppose to the contrary that $g(0) \notin \mathfrak{p}$; and suppose $h(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_\ell x^\ell \pmod{\mathfrak{p}}$ and $b_\ell \notin \mathfrak{p}$. Notice that $\ell \leq m < n$.

So $g(0)\, b_\ell\, x^\ell$ is a term of $g(x)\, h(x) \pmod{\mathfrak{p}}$, which contradicts (1). $\square$ (claim)

So $a_0 = f(0) = g(0)\, h(0) \in \mathfrak{p}^2$ which is a contradiction. $\blacksquare$

<u>Remark.</u> For any integral domain D and $\theta \in \mathrm{Aut}(D)$, if d is irreducible in D, then $\theta(d)$ is also irred. So $f(x) \in D[x]$ is irreducible if and only if $f(x-a)$ is irred. for some $a \in D$. In some examples one can use Eisentein's criterion for $f(x-a)$ and a good choice of a.

Lecture 02: Special case of cyclotomic polynomials

Saturday, January 12, 2019 12:08 AM

Ex. Show that $x^{p-1}+x^{p-2}+\cdots+1$ is irreducible in $\mathbb{Q}[x]$ if p is prime.

Pf. Let $f(x)=x^{p-1}+\cdots+1=\dfrac{x^p-1}{x-1}$. Hence

$$f(x+1)=\frac{(x+1)^p-1}{x}=x^{p-1}+\binom{p}{p-1}x^{p-2}+\cdots+\binom{p}{1}.$$

Notice that $\left.\begin{array}{l}\binom{p}{i}=\dfrac{p(p-1)\cdots(p-i+1)}{i!}\\ p\nmid i! \quad \text{for } 1\le i\le p-1\end{array}\right\}\Rightarrow p\mid\binom{p}{i}$,

and $p^2\nmid p=\binom{p}{1}$. Hence by Eisenstein's criterion $f(x+1)$ is irreducible in $\mathbb{Z}[x]$; And so $f(x)$ is irreducible in $\mathbb{Z}[x]$. Since $\deg f\ge 1$, $\mathbb{Z}$ is a UFD, and f is primitive, we deduce that $f(x)$ is irreducible in $\mathbb{Q}[x]$. ∎

Remark. The above example is a special case of cyclotomic polynomials: $q_n(x):=\prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}}(x-\zeta_n^k)$ where $\zeta_n=e^{\frac{2\pi i}{n}}$.

We will show that $q_n(x)\in\mathbb{Z}[x]$ and it is irred. in $\mathbb{Q}[x]$.

One can see that $q_p(x)=\prod_{1\le k\le p-1}(x-\zeta_n^k)=\dfrac{x^p-1}{x-1}$; and so the above example is a special case of this statement.

Lecture 02: Localization

Saturday, January 12, 2019 12:21 AM

Suppose A is a unital commutative ring and $S \subseteq A$ is a multiplicatively closed subset. We would like to consider a ring consisting of "fractions" $\frac{a}{s}$ where $s \in S$.

For $(a_1, s_1), (a_2, s_2) \in A \times S$, we say $(a_1, s_1) \sim (a_2, s_2)$ if $\exists\, s \in S$ s.t. $s(s_2 a_1 - s_1 a_2) = 0$.

<u>Claim</u>. $\sim$ is an equivalence relation.

<u>pf of Claim</u>. One can easily see $(a, s) \sim (a, s)$ and $(a_1, s_1) \sim (a_2, s_2) \Rightarrow (a_2, s_2) \sim (a_1, s_1)$. So we focus on transitive property:

$$\left.\begin{array}{l}(a_1, s_1) \sim (a_2, s_2)\\ (a_2, s_2) \sim (a_3, s_3)\end{array}\right\} \overset{?}{\Rightarrow} (a_1, s_1) \sim (a_3, s_3).$$

$(a_1, s_1) \sim (a_2, s_2) \Rightarrow \exists\, s \in S,\ s(a_1 s_2 - a_2 s_1) = 0$ ①

$(a_2, s_2) \sim (a_3, s_3) \Rightarrow \exists\, s' \in S,\ s'(a_2 s_3 - a_3 s_2) = 0$ ②

$$\left.\begin{array}{l}① \Rightarrow s's(s_3 a_1 s_2 - s_3 a_2 s_1) = 0\\ ② \Rightarrow s's(s_1 a_2 s_3 - s_1 a_3 s_2) = 0\end{array}\right\} \Rightarrow s's(s_3 a_1 s_2 - s_1 a_3 s_2) = 0 \Rightarrow \underbrace{s's s_2}_{\text{in } S}(s_3 a_1 - s_1 a_3) = 0$$

$\Rightarrow (a_1, s_1) \sim (a_3, s_3)$.

Lecture 02: Localization

Saturday, January 12, 2019 12:32 AM

We let $\frac{a}{s} := [(a,s)]_{\sim}$ and define $+, \cdot$ similar to fractions in $\mathbb{Q}$. One can easily see that $S^{-1}A$ is a ring. Let $f: A \to S^{-1}A$, $f(a) := \frac{a}{1}$. One can see that f is a ring hom. It is not necessarily injective.

$$a \in \ker f \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists s \in S,\ s(a-0)=0$$

$$\Leftrightarrow \exists s \in S,\ sa = 0$$

So $\ker f = \{a \in A \mid \exists s,\ as=0\}$; in particular f is injective if and only if S does not contain any zero-divisor (and 0).

Notice $S^{-1}A = 0 \Leftrightarrow 0 \in S$.

- For any $\mathfrak{p} \in \operatorname{Spec} A$, $S_{\mathfrak{p}} := A \setminus \mathfrak{p}$ is a multiplicatively closed set: • $\mathfrak{p}$ is proper $\Rightarrow 1 \notin \mathfrak{p} \Rightarrow 1 \in S_{\mathfrak{p}}$

  • $a, b \in S_{\mathfrak{p}} \Rightarrow a, b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p} \Rightarrow ab \in S_{\mathfrak{p}}$.

$S_{\mathfrak{p}}^{-1}A$ is denoted by $A_{\mathfrak{p}}$; and it is called the localization of A at $\mathfrak{p}$.

Lecture 02: Localization

Saturday, January 12, 2019 12:42 AM

<u>Theorem</u> (Universal property of localization)

Suppose A and B are unital commutative rings, $S \subseteq A$ is a multiplicatively closed subset, and $\theta: A \to B$ is a ring hom. s.t. $\theta(S) \subseteq B^\times$. Then $\exists!\ \hat{\theta}: S^{-1}A \to B$ s.t. $\hat{\theta}\left(\frac{a}{1}\right) = \theta(a)$.

$$\begin{tikzcd} A \arrow[r, "\theta"] \arrow[d, "f"'] & B \\ S^{-1}A \arrow[ur, dashed, "\hat{\theta}"'] \arrow[u, phantom, shift left=4ex, "\circlearrowleft"] & \end{tikzcd}$$

<u>Pf.</u> We start with uniqueness to find out what $\hat{\theta}$ should be which helps us to show existence.

For $s \in S$, $\left.\begin{aligned} &\hat{\theta}\left(\tfrac{1}{s}\right) \cdot \hat{\theta}\left(\tfrac{s}{1}\right) = \hat{\theta}\left(\tfrac{1}{1}\right) = 1 \\ &\hat{\theta}\left(\tfrac{s}{1}\right) = \theta(s) \end{aligned}\right\} \Rightarrow \hat{\theta}\left(\frac{1}{s}\right) = \theta(s)^{-1}$.

$$\Rightarrow \hat{\theta}\left(\frac{a}{s}\right) = \hat{\theta}\left(\frac{a}{1}\right) \cdot \hat{\theta}\left(\frac{1}{s}\right) = \theta(s)^{-1}\theta(a).$$

This implies the uniqueness. . Let $\hat{\theta}\left(\frac{a}{s}\right) := \theta(s)^{-1}\theta(a)$;

. <u>$\hat{\theta}$ is well-defined.</u> $\quad \frac{a_1}{s_1} = \frac{a_2}{s_2} \Rightarrow \exists s \in S,\ s(a_1 s_2 - a_2 s_1) = 0$

$$\Rightarrow \theta(s)\left(\theta(a_1)\theta(s_2) - \theta(a_2)\theta(s_1)\right) = 0 \qquad (\theta(s), \theta(s_i) \in B^\times)$$

$$\Rightarrow \theta(s_1)^{-1}\theta(a_1) = \theta(s_2)^{-1}\theta(a_2).$$

One can easily check that $\hat{\theta}$ is a ring hom., which implies the existence. ∎

Lecture 02: Module theory

Saturday, January 12, 2019 1:49 AM

Similar to groups, the best way of understanding rings it is best to let it act; here we are more or less forced to consider linear actions.

Let A be a unital ring; we say M is a left A-module if

- M is an abelian group
- $\exists \cdot : A \times M \to M$, $(a,m) \mapsto a\cdot m$ with the following properties:
  - (P0) $1\cdot m = m$
  - (P1) $(a_1+a_2)\cdot m = a_1\cdot m + a_2\cdot m$
  - (P2) $a\cdot(m_1+m_2) = a\cdot m_1 + a\cdot m_2$
  - (P3) $a_1\cdot(a_2\cdot m) = (a_1a_2)\cdot m$

Similarly we can defined a right A-mod.

$\boxed{Q}$ Given a left A-module, can we get a right module?

We naïvely define $m * a := a\cdot m$.

(P1) and (P2) are satisfied.

$$(m*a_1)*a_2 = (a_1\cdot m)*a_2 = a_2\cdot(a_1\cdot m) = (a_2a_1)\cdot m$$
$$= m*(a_2a_1).$$

Since a_2a_1 is not necessarily a_1a_2, (P3) does not necessarily hold. Let A^{op} be the opposite ring of A; $(A^{op},+)=(A,+)$ and $a\cdot a' := a'a$. Then by the above computation we have that any left A-module M is a right A^{op}-module and vice versa.

A few examples:

1. Suppose A is a unital ring; $I \subseteq A$ is called a left ideal if $\forall\, x,y\in I,\ x-y\in I$, $\forall\, x\in I, a\in A,\ ax\in I$.

Then I is a left A-module: $a\cdot x := ax$.

2. A: unital ring; $I\subseteq A$: left ideal $\Rightarrow A/I$ is a left A-mod.: $a(x+I) := ax+I$

<u>Well-defined</u>. $x_1+I = x_2+I \Rightarrow x_2 = x_1 + x$ for some $x\in I$

$$\Rightarrow ax_2 = ax_1 + \underbrace{ax}_{\text{in } I} \Rightarrow ax_2 + I = ax_1 + I.$$

One can check all the properties easily.

3. Suppose $M_1,\dots,M_n$ are left A-mod. Then $M_1\oplus\cdots\oplus M_n$ is a left A-mod, $a\cdot(x_1,\dots,x_n) := (ax_1,\dots,a\cdot x_n)$. In particular A^n is a left A-mod.

Lecture 02: Module theory

Saturday, January 12, 2019 2:17 AM

4. A^n is a left $M_n(A)$-module;

$$\forall\ [a_{ij}] \in M_n(A),\ \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \quad [a_{ij}]\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} := \Big[\sum_{j=1}^{n} a_{ij}\, b_j\Big].$$

5. (Induced module structure) Similar to the group actions

$$\left.\begin{array}{l} G \curvearrowright X \\ H \xrightarrow[\theta]{} G \end{array}\right\} \Rightarrow H \curvearrowright X,\ h * x := \theta(h)\cdot x.$$ We can defined

an induced module structure: suppose A and B are unital rings and $\theta : B \to A$ is a ring hom. Suppose M is a left A-mod. Then $b * m := \theta(b)\, m$ makes M into a left B-mod.

6. If B is a subring of A and M is an A-mod, then M is a left B-mod; ($B \hookrightarrow A$ and induced mod. structure.)

7. $I \trianglelefteq A \Rightarrow$ any left A/I-mod can be viewed as an A-mod. ($A \to A/I$ and induced mod.)

8. Suppose A is a commutative unital ring, $a \in A$, and M is a left A-mod. Let $\theta_a : A[x] \to A$ be the evaluation at a map. So M can be viewed as a left $A[x]$-module.