Lecture 14: How to use irreducible elements to show certain ring is not a PID

Monday, May 7, 2018 11:28 AM

- $\sqrt{-6}$ is irreducible in $\mathbb{Z}[\sqrt{-6}]$.

<u>Pf.</u> . $\sqrt{-6} \neq 0$

. Since $\mathbb{Z}[\sqrt{-6}]$ is a subring of $\mathbb{C}$, it has no zero-divisors.

. $\sqrt{-6}$ is not unit; otherwise $\exists\, a, b \in \mathbb{Z}$ s.t.

$$(\sqrt{-6})(a+b\sqrt{-6}) = 1.$$

Hence considering the square of the complex norm we deduce

$$|\sqrt{-6}|^2 \, |a+b\sqrt{-6}|^2 = 1^2 \Rightarrow (6)\underbrace{(a^2+6b^2)}_{\text{in } \mathbb{Z}} = 1$$

$\Rightarrow 6 \mid 1$ which is a contradiction.

. $\sqrt{-6} = (a+b\sqrt{-6})(c+d\sqrt{-6}) \Rightarrow |\sqrt{-6}|^2 = |a+b\sqrt{-6}|^2 \, |c+d\sqrt{-6}|^2$

$$\Rightarrow 6 = \underbrace{(a^2+6b^2)}_{\in \mathbb{Z}^{\geq 0}} (c^2+6d^2) \Rightarrow$$

$a^2+6b^2 = 1$, or 2, or 3, 6.

. <u>Notice</u> If $b \neq 0$, then $6b^2 \geq 6 \Rightarrow a^2+6b^2 \geq 6$. $(*)$

<u>Claim</u>. $a^2+6b^2 \neq 2$ and $a^2+6b^2 \neq 3$.

<u>If not</u>, then $a^2+6b^2 < 6$; and so by $(*)$ $b=0$. Then $a^2=2$ or $a^2=3$, which is a contrad. as 2 and 3 are not perfect square.

Lecture 14: How to use irreducible elements to show certain ring is not a PID

Monday, May 7, 2018 11:38 AM

By this claim, either $a^2+6b^2=1$ or $c^2+6d^2=1$. W.L.O.G

let's assume $a^2+6b^2=1$.

<u>Claim</u>. $a+\sqrt{-6}\, b$ is a unit.

<u>Pf</u>. $1=a^2+6b^2=(a+\sqrt{-6}\,b)\underbrace{(a-\sqrt{-6}\,b)}_{\text{in } \mathbb{Z}[\sqrt{-6}]}$

Hence $a+\sqrt{-6}\,b$ is a unit in $\mathbb{Z}[\sqrt{-6}]$.

Therefore $\sqrt{-6}$ is irreducible. ∎

<u>Proposition</u> $\mathbb{Z}[\sqrt{-6}]$ is not a PID.

<u>Pf</u>. Suppose to the contrary that $\mathbb{Z}[\sqrt{-6}]$ is a PID. Then since $\sqrt{-6}$ is irreducible, $\langle\sqrt{-6}\rangle$ is a maximal ideal of $\mathbb{Z}[\sqrt{-6}]$. Hence $\langle\sqrt{-6}\rangle$ is a prime ideal of $\mathbb{Z}[\sqrt{-6}]$.

<u>Claim</u>. $(-2)(3)\in\langle\sqrt{-6}\rangle$ and $-2\notin\langle\sqrt{-6}\rangle$ and $3\notin\sqrt{-6}$.

<u>Pf of claim</u>. $(-2)(3)=-6=\sqrt{-6}\cdot\sqrt{-6}\in\langle\sqrt{-6}\rangle$.

If $-2\in\langle\sqrt{-6}\rangle$, then $-2=\sqrt{-6}\,(a+b\sqrt{-6})=\sqrt{-6}\,a-6b$;

Comparing real parts, we deduce $-2=-6b \Rightarrow b=1/3$ which is a contradiction as $b \in \mathbb{Z}$.

. If $3 \in \langle \sqrt{-6} \rangle$, then $3 = \sqrt{-6}\,(a+b\sqrt{-6})$ for some $a, b \in \mathbb{Z}$.

Hence $3 = \sqrt{-6}\, a - 6b$. Comparing the real parts, $3 = -6b$; and so

$b = -\frac{1}{2}$ which is a contradiction as $b \in \mathbb{Z}$.

And so $\langle \sqrt{-6} \rangle$ is not a prime ideal; this implies $\mathbb{Z}[\sqrt{-6}]$ is not a PID. ∎

Next we go back to polynomials and zeros of polynomials. Suppose $\alpha \in \mathbb{C}$. Then the evaluation at α gives us a ring homomorphism $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$, $\phi_\alpha(f(x)) = f(\alpha)$. We have seen examples of this and how helpful ϕ_α can be. In general,

$$\ker \phi_\alpha = \{ f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0 \} = \{ f(x) \in \mathbb{Q}[x] \mid \alpha \text{ is a zero of } f \}.$$

For many α's, $\ker \phi_\alpha = \{0\}$. This takes us to the next def.

<u>Def.</u> $\alpha \in \mathbb{C}$ is called an algebraic number if α is a zero of a non-zero polynomial; alternatively if $\ker \phi_\alpha \neq \{0\}$.

. $\alpha \in \mathbb{C}$ is called transcendental if it is not algebraic.

Lecture 14: Minimal polynomial

Wednesday, May 9, 2018 10:47 PM

Theorem. Suppose $\alpha \in \mathbb{C}$ is an algebraic number. Then

$\exists\, m_\alpha(x) \in \mathbb{Q}[x]$ s.t.

(1) $\ker \phi_\alpha = \langle m_\alpha(x) \rangle$ (2) $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$.

(Such $m_\alpha(x)$ is called a minimal polynomial of α over $\mathbb{Q}$.)

Pf ① Since $\mathbb{Q}[x]$ is a PID, $\exists\, m_\alpha(x) \in \mathbb{Q}[x]$ s.t. $\ker \phi_\alpha = \langle m_\alpha(x) \rangle$.

②. Since α is algebraic, $\ker \phi_\alpha \neq 0$. And so $m_\alpha(x) \neq 0$.

. As $\mathbb{Q}[x]$ is an integral domain, $m_\alpha(x)$ is not a zero-divisor.

. If $m_\alpha(x)$ is a unit, then $\ker \phi_\alpha = \mathbb{Q}[x]$; and so $1 \in \ker \phi_\alpha$ which is a contradiction as 1 does not have a zero.

. $m_\alpha(x) = a(x)\, b(x) \Rightarrow m_\alpha(\alpha) = a(\alpha)\, b(\alpha) \Rightarrow a(\alpha)\, b(\alpha) = 0$

$\Rightarrow$ either $a(\alpha) = 0$ or $b(\alpha) = 0$; w.l.o.g. let's assume $a(\alpha) = 0$

$\Rightarrow a(x) \in \ker \phi_\alpha = \langle m_\alpha(x) \rangle \Rightarrow a(x) = m_\alpha(x)\, q(x)$ for some $q(x) \in \mathbb{Q}[x]$. Hence $m_\alpha(x) = m_\alpha(x)\, q(x)\, b(x)$. Since $\mathbb{Q}[x]$ is an integral domain, by the cancelation law $1 = q(x)\, b(x)$.

And so $b(x) \in U(\mathbb{Q}[x])$. Therefore $m_\alpha(x)$ is irreducible. ∎

Lecture 14: Minimal polynomial

Wednesday, May 9, 2018 11:05 PM

<u>Remark</u>.. One can see that $\mathbb{Q}[x]$ is an integral domain using

$$\deg fg = \deg f + \deg g,$$

we will generalize this later.

- $m_\alpha(x)$ is a minimal poly. of α over $\mathbb{Q}$ if
  - $m_\alpha(\alpha) = 0$
  - $m_\alpha(x)$ is the smallest degree poly. that has α as a zero.

- $m_\alpha(x)$ is a minimal poly. of α over $\mathbb{Q}$ if

  $f(\alpha) = 0 \iff m_\alpha(x) \mid f(x)$.