The fundamental homomorphism theorem

Friday, August 25, 2017 12:52 AM

<u>Theorem</u>. Suppose $\phi: R \to S$ is a ring homomorphism.

Then ① $\mathrm{Im}(\phi)$ is a subring of S. (the image of ϕ)

② $\ker(\phi)$ is an ideal of R.

③ $\bar{\Phi}: R/_{\ker(\phi)} \to \mathrm{Im}(\phi)$,

$$\bar{\Phi}(r+\ker\phi) = \phi(r)$$

is a ring isomorphism.

<u>Proof</u>. ① Since ϕ is a group homomorphism of $(R,+)$, $\mathrm{Im}(\phi)$ is a subgroup of $(S,+)$. So to show it is a subring, it is enough to show it is closed under multiplication:

$\forall y_1, y_2 \in \mathrm{Im}(\phi)$, $\exists r_1, r_2 \in R$, $y_1 = \phi(r_1)$ and $y_2 = \phi(r_2)$.

So $y_1 y_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2)$, which implies

$y_1 y_2 \in \mathrm{Im}\,\phi$.

② We have already proved.

③ In group theory, you have seen that $\bar{\Phi}$ is a well-defined group isomorphism from $(R/_{\ker\phi}, +)$ to $(\mathrm{Im}\,\phi, +)$. So it is enough to prove $\bar{\Phi}$ preserves multiplication. But

The fundamental homomorphism theorem

Friday, August 25, 2017 1:02 AM

For the sake of completeness, let's recall the group theory part:

<u>well-definedness</u>. $r_1 + \ker\phi = r_2 + \ker\phi \overset{?}{\Rightarrow} \phi(r_1) = \phi(r_2)$

$r_1 + \ker\phi = r_2 + \ker\phi \Rightarrow r_1 - r_2 \in \ker\phi$

$\Rightarrow \phi(r_1 - r_2) = 0$

$\Rightarrow \phi(r_1) = \phi(r_2)$.

<u>Injective</u>. $\overline{\Phi}(r_1 + \ker\phi) = \overline{\Phi}(r_2 + \ker\phi) \Rightarrow \phi(r_1) = \phi(r_2)$

$\Rightarrow \phi(r_1 - r_2) = 0$

$\Rightarrow r_1 - r_2 \in \ker\phi \Rightarrow r_1 + \ker\phi = r_2 + \ker\phi$.

<u>Surjective</u>. $\forall\, y \in \operatorname{Im}\phi, \exists\, r \in R,\ y = \phi(r)$

$\Rightarrow y = \overline{\Phi}(r + \ker\phi)$.

<u>Preserves addition</u> is similar to next step. (Do it on your own.)

<u>Preserves multiplication</u> $\overline{\Phi}((r_1 + \ker\phi)\cdot(r_2 + \ker\phi))$

Examples

Friday, August 25, 2017 1:12 AM

Ex. Prove that $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ as two rings.

Pf. Let $c_n : \mathbb{Z} \to \mathbb{Z}_n$ be the residue homomorphism.

Then $c_n(i) = i$ if $0 \le i < n$. So $\operatorname{Im} c_n = \mathbb{Z}_n$. And

$a \in \ker c_n \iff$ the remainder of a divided by n is 0

$$\iff n \mid a \iff a \in n\mathbb{Z}.$$

So by the fundamental homomorphism theorem,

$$\bar{c}_n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n, \quad \bar{c}_n(a + n\mathbb{Z}) = c_n(a)$$

is a ring isomorphism. ∎

Ex ⓐ Prove that the kernel of the evaluation homomorphism

$$\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}, \quad \phi_{\sqrt{2}}(f(x)) = f(\sqrt{2})$$

is $\langle x^2 - 2 \rangle$.

ⓑ Prove that $\operatorname{Im} \phi_{\sqrt{2}} = \mathbb{Q}[\sqrt{2}]$.

ⓒ Deduce that $\mathbb{Q}[x]/\langle x^2-2 \rangle \simeq \mathbb{Q}[\sqrt{2}]$.

Pf. ⓐ Since $\mathbb{Q}[x]$ is a PID, $\exists\, f_0(x) \in \mathbb{Q}[x]$ such that

$$\langle f_0(x) \rangle = \ker \phi_{\sqrt{2}}.$$

On the other hand, $\phi_{\sqrt{2}}(x^2-2) = (\sqrt{2})^2 - 2 = 0$; so $x^2 - 2 \in \langle f_0(x) \rangle$.

Examples

Sunday, August 27, 2017 8:32 PM

which implies $f_0(x)\,q(x) = x^2-2$ for some $q(x) \in \mathbb{Q}[x]$.

Since $\pm\sqrt{2} \notin \mathbb{Q}$, x^2-2 has no zero in $\mathbb{Q}$. As x^2-2 is of degree 2 and it does not have a zero in $\mathbb{Q}$, x^2-2 is irreducible in $\mathbb{Q}[x]$. The irreducibility of x^2-2 and $f_0(x)q(x)=x^2-2$, implies either $\deg f_0 = 0$ or $\deg q = 0$.

If $\deg f_0 = 0$, then $\langle f_0(x)\rangle = \mathbb{Q}[x]$; which is not possible as $\phi_{\sqrt{2}}(1) = 1 \neq 0$. Hence $\deg q = 0$; this implies

$$\langle x^2-2\rangle = \langle f_0(x)\rangle = \ker \phi_{\sqrt{2}}.$$

(b) In an example earlier we have seen that $\mathbb{Q}[\sqrt{2}]$ is a field. In particular, for any $a_i \in \mathbb{Q}$ we have

$$a_0 + a_1\sqrt{2} + \cdots + a_n(\sqrt{2})^n \in \mathbb{Q}[\sqrt{2}].$$

Therefore $\forall f(x) \in \mathbb{Q}[x]$, $\phi_{\sqrt{2}}(f) \in \mathbb{Q}[\sqrt{2}]$; this implies $\operatorname{Im} \phi_{\sqrt{2}} \subseteq \mathbb{Q}[\sqrt{2}]$. I

On the other hand, for any $a, b \in \mathbb{Q}$, $\phi_{\sqrt{2}}(a+bx) = a + b\sqrt{2}$; and so $\mathbb{Q}[\sqrt{2}] \subseteq \operatorname{Im} \phi_{\sqrt{2}}$. II. I, II imply the claim.

Examples; Evaluation at an algebraic number

Sunday, August 27, 2017 8:46 PM

(c) By the fundamental homomorphism theorem, we have

$$\mathbb{Q}[x]/\ker\phi_{\sqrt{2}} \simeq \operatorname{Im}\phi_{\sqrt{2}}; \text{ and so}$$

$$\mathbb{Q}[x]/\langle x^2-2\rangle \simeq \mathbb{Q}[\sqrt{2}].$$ ■

A closer look at the previous example gives us several results.

Theorem. Suppose $\alpha \in \mathbb{C}$ is an algebraic number; this means α is a zero of a polynomial $f_1(x) \in \mathbb{Q}[x]\setminus\{0\}$. Let $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ be the evalution at α map; that means $\phi_\alpha(f) = f(\alpha)$. Then

1. there is an irreducible polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ such that $\ker\phi_\alpha = \langle m_\alpha(x)\rangle$.
2. $\operatorname{Im}\phi_\alpha = \{a_0 + a_1\alpha + \cdots + a_{k_0}\alpha^{k_0} \mid a_i \in \mathbb{Q}\}$ where $k_0 = \deg m_\alpha - 1$.
3. $\operatorname{Im}\phi_\alpha$ is a field. (We will prove later)

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

Evaluation at an algebraic number

Sunday, August 27, 2017 9:08 PM

Claim $m_\alpha(x)$ is irreducible.

Pf of claim. Suppose $m_\alpha(x) = f(x)\,g(x)$ for some $f, g \in \mathbb{Q}[x]$.

Then $0 = m_\alpha(\alpha) = f(\alpha)\,g(\alpha)$. Since $\mathbb{C}$ has no zero divisor, either $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, let's assume $f(\alpha) = 0$. So $f \in \ker \phi_\alpha = \langle m_\alpha(x) \rangle$; this implies

$$f(x) = m_\alpha(x)\,q(x) \text{ for some } q \in \mathbb{Q}[x].$$

Hence $\deg f \le \deg m_\alpha \le \deg f$, which implies $\deg g = 0$. Therefore $m_\alpha(x)$ is irreducible in $\mathbb{Q}[x]$.

② Suppose $a \in \operatorname{Im}(\phi_\alpha)$. Then $a = \phi_\alpha(f) = f(\alpha)$ for some $f \in \mathbb{Q}[x] \setminus \ker \phi_\alpha$. By the division algorithm $\exists\, q, r \in \mathbb{Q}[x]$ such that ① $f(x) = m_\alpha(x)\,q(x) + r(x)$, and

② $\deg r < \deg m_\alpha = k_0 + 1$.

So $a = f(\alpha) = \underbrace{m_\alpha(\alpha)}_{0}\,q(\alpha) + r(\alpha) = r(\alpha)$

Since $\deg r \le k_0$, $\exists\, a_i \in \mathbb{Q}$ s.t. $r(x) = a_0 + a_1 x + \cdots + a_{k_0} x^{k_0}$; this implies $a = a_0 + a_1\alpha + \cdots + a_{k_0}\alpha^{k_0}$ for some $a_i \in \mathbb{Q}$. ∎