Lecture 13: Ideals; kernels of ring homomorphisms

Thursday, August 24, 2017 11:57 PM

We have seen that $\underline{\ker}\ \phi_\alpha$ is an ideal; next we see that kernel of any ring homomorphism is an ideal. In fact we will see

$$\boxed{I \text{ is an ideal of } R \text{ if and only if there is a ring homomorphism } \phi: R \to R' \text{ such that } \ker(\phi) = I.}$$

Let's start by proving $(\Leftarrow)$.

<u>Lemma</u>. Suppose $\phi: R \to R'$ is a ring homomorphism. Then $\ker \phi$ is an ideal of R.

<u>Proof</u>. For $r_1, r_2 \in \ker \phi$, $\phi(r_1) = \phi(r_2) = 0$; and so $\phi(r_1+r_2) = \phi(r_1) + \phi(r_2) = 0$, which implies $r_1 + r_2 \in \ker \phi$.

Now suppose $x \in \ker \phi$ and $r \in R$.

ϕ is a ring homomorphism

Then $\phi(rx) = \phi(r)\phi(x)$

$x \in \ker \phi$

$= (\phi(r))(0) = 0$.

(Similarly we can show $\phi(xr) = 0$; but in this course we are working with commutative rings, and so it is not necessary.) ∎

Lecture 13: The quotient ring

Friday, August 25, 2017 12:10 AM

Next starting with an ideal I of R, we will construct the quotient ring of R by I:

Lemma. Suppose $I \triangleleft R$. Let $(x+I)\cdot(y+I) = xy+I$. Then this is a well-defined binary operation on $R/_I$ and $(R/_I, +, \cdot)$ is a ring. (It is called the quotient ring of R by I.)

Before we prove this lemma, let's recall the group theoretic counterpart of this concept. For a group G, a subgroup N is called a normal subgroup if, for any $g \in G$, $gN = Ng$.

In group theory, you have seen that, if N is a normal subgp of G, then $(g_1 N)\cdot(g_2 N) = g_1 g_2 N$ defines a well-defined binary operation on the set $G/_N$ of (left) cosets of N in G. And $(G/_N, \cdot)$ is a group.

Since, for a ring R, $(R,+)$ is an abelian group, any subgroup is a normal subgroup; so $(R/_I, +)$ is a group

Lecture 13: The quotient ring

Friday, August 25, 2017 12:23 AM

if I is an ideal of R.

Let's also recall that if $(A,+)$ is an abelian group and N is a subgroup, then $a+N = a'+N \Leftrightarrow a-a' \in N$.

($(\Rightarrow)$ $a' \in a+N \Rightarrow a' = a+x$ for some $x \in N$

$\Rightarrow a - a' = -x \in N$

$(\Leftarrow)$ $a+N = a' + \underbrace{(a-a') + N}_{N \text{ as } a-a' \in N \text{ and } N \text{ is a subgroup.}} = a'+N$)

Proof of Lemma.

Well-definedness. $\left.\begin{matrix} x_1+I = x_2+I \\ y_1+I = y_2+I \end{matrix}\right\} \overset{?}{\Longrightarrow} x_1y_1 + I = x_2y_2 + I.$

Pf. From group theory we know that

$$x_1y_1 + I = x_2y_2 + I \Leftrightarrow x_1y_1 - x_2y_2 \in I;$$

$$x_1 + I = x_2 + I \Rightarrow x_1 - x_2 \in I \quad (1)$$

$$y_1 + I = y_2 + I \Rightarrow y_1 - y_2 \in I \quad (2)$$

We have $$x_1y_1 - x_2y_2 = x_1y_1 - x_2y_1 + x_2y_1 - x_2y_2$$

$$= \underbrace{(x_1-x_2)}_{\text{in } I \text{ by } (1)} y_1 + x_2 \underbrace{(y_1-y_2)}_{\text{in } I \text{ by } (2)} \in I$$

Lecture 13: The quotient ring

Friday, August 25, 2017 12:36 AM

The distributive property and the associativity can be deduced from the fact that R is a ring. ∎

<u>Lemma</u>. Suppose I is an ideal of a ring R. Then

$$\pi : R \to R/I, \quad \pi(r) = r + I$$

is a surjective ring homomorphism; and $\ker \pi = I$.

(we call π the <u>natural quotient map</u>.)

<u>Pf.</u> From group theory, we know that π is a surjective group homomorphism of $(R,+)$ to $(R/I,+)$; and $\ker \pi = I$.

So it is enough to check that π preserves multiplication:

$$\pi(r_1)\cdot\pi(r_2) = (r_1+I)\cdot(r_2+I) = r_1r_2 + I = \pi(r_1r_2),$$

and the claim follows. ∎

These lemmas show us that

$$I \text{ is an ideal of } R \iff \exists \text{ a ring homomorphism } \phi: R \to R' \text{ such that } \ker\phi = I.$$

Next we prove the 1st isomorphism theorem, in your book it is called the fundamental homomorphism theorem.

<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 $\overline{\phi}: R/\ker(\phi) \to \mathrm{Im}(\phi)$, $\overline{\phi}(r+\ker\phi) = \phi(r)$

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 $\overline{\phi}$ is a well-defined group isomorphism from $(R/\ker\phi, +)$ to $(\mathrm{Im}\,\phi, +)$. So it is enough to prove $\overline{\phi}$ preserves multiplication. But

Lecture 13: 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>. $r_1 + \ker\phi = r_2 + \ker\phi \overset{?}{\Longrightarrow} \phi(r_1) = \phi(r_2)$

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

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

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

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

$= \overline{\Phi}(r_1 r_2 + \ker\phi) = \phi(r_1 r_2)$

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

$= \overline{\Phi}(r_1 + \ker\phi)\, \overline{\Phi}(r_2 + \ker\phi)$. ∎

Lecture 13: 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

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

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

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 $(x^2-2)\mathbb{Q}[x]$.

ⓑ Prove that $\operatorname{Im} \phi_{\sqrt{2}} = \mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$.

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

Pf. ⓐ Suppose $m_{\sqrt{2}}(x) \in \mathbb{Q}[x]$ is the minimal poly. of $\sqrt{2}$ over $\mathbb{Q}$; and so $\ker \phi_{\sqrt{2}} = m_{\sqrt{2}}(x)\mathbb{Q}[x]$.

On the other hand, $\phi_{\sqrt{2}}(x^2-2) = (\sqrt{2})^2 - 2 = 0$; so $m_{\sqrt{2}}(x) \mid x^2 - 2$.

Lecture 13: Examples

Sunday, August 27, 2017 8:32 PM

On the other hand, x^2-2 is irreducible in $\mathbb{Q}[x]$ (either use Eisenstein's criterion or the fact that x^2-2 has no zero in in $\mathbb{Q}$ as $\pm\sqrt{2}\notin\mathbb{Q}$ and it has degree 2.) The irreducibility of x^2-2 and $m_{\sqrt{2}}(x) \mid x^2-2$, implies either $m_{\sqrt{2}}(x)$ is a unit or $m_{\sqrt{2}}(x) = x^2-2$ (as they are both monic).

If $m_{\sqrt{2}}(x)$ is a unit, $\ker\phi_{\sqrt{2}} = \mathbb{Q}[x]$; which is not possible as $\phi_{\sqrt{2}}(1) = 1 \neq 0$. Hence

$$\ker\phi_{\sqrt{2}} = m_{\sqrt{2}}(x)\,\mathbb{Q}[x] = (x^2-2)\,\mathbb{Q}[x].$$

(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.

Lecture 13: Evaluation at an algebraic number

Sunday, August 27, 2017 8:46 PM

(c) By the fundamental homomorphism theorem, we have

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

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

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

Proposition. 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 $\ker \phi_\alpha = m_\alpha(x)\mathbb{Q}[x]$
2. $\operatorname{Im} \phi_\alpha = \mathbb{Q}[\alpha]$ is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ as a subset and α as an element and $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_m\alpha^m \mid a_i \in \mathbb{Q}, m \in \mathbb{Z}^+\}$.
3. $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x] \simeq \mathbb{Q}[\alpha]$.

Pf. Let $m_\alpha(x) \in \mathbb{Q}[x]$ be the minimal poly. of α over $\mathbb{Q}$.

Lecture 13: Evaluation at an algebraic number

Sunday, August 27, 2017 9:08 PM

<u>Claim</u> $m_\alpha(x)$ is irreducible.

<u>Pf of claim.</u> Since $m_\alpha(x)$ is monic, it is not zero. As $1 \notin \ker \phi_\alpha$, $\deg m_\alpha \geq 1$. 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 $f \in \ker \phi_\alpha = m_\alpha(x)\mathbb{Q}[x]$; this implies

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

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

- $\operatorname{Im} \phi_\alpha = \{ f(\alpha) \mid f(x) \in \mathbb{Q}[x] \} = \{ a_0 + a_1\alpha + \cdots + a_m \alpha^m \mid a_i \in \mathbb{Q}, m \in \mathbb{Z}^+ \}$.

If $A \subseteq \mathbb{C}$ is a subring, $\mathbb{Q} \subseteq A$, and $\alpha \in A$, then for any $i \in \mathbb{Z}^+$

$$\left.\begin{array}{l} \underbrace{\alpha \cdot \alpha \cdot \cdots \cdot \alpha}_{i} = \alpha^i \in A \\ a_i \in \mathbb{Q} \subseteq A \end{array}\right\} \Rightarrow a_i \alpha^i \in A \Rightarrow \sum_{i=0}^{m} a_i \alpha^i \in A$$

$\Rightarrow \operatorname{Im} \phi_\alpha \subseteq A$. Hence $\operatorname{Im} \phi_\alpha$ is the smallest subring of $\mathbb{C}$ that has α as an element and $\mathbb{Q}$ as a subset.

Lecture 13: Evaluation at an algebraic number; prime

Saturday, February 23, 2019 10:35 PM

- Consider the ring homomorphism $\phi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$; by the 1st isomorphism theorem

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

$$\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x] \simeq \mathbb{Q}[\alpha].$$

Next we would like to show $\mathbb{Q}[\alpha]$ is a field; you have seen very special cases of this statement: $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, and $\mathbb{Q}[\omega]$ are fields.

To prove this, we will find out the necessary and sufficient conditions for $I \trianglelefteq R$ such that R/I is an integral domain or a field.

We start with the easier case: under what conditions is R/I an integral domain?

Investigation. Since R is a unital commutative ring,

R/I is an integral domain $\Leftrightarrow$ ① $R/I \neq 0$

② R/I does not have a zero divisor

Lecture 13: Prime and maximal ideals

Sunday, August 27, 2017 10:19 PM

$\Leftrightarrow$ ① $R \neq I$.

② $(x+I)(y+I) = (0+I)$ implies either $x+I = 0+I$

or $y+I = 0+I$

$\Leftrightarrow$ ① I is a proper ideal ② $xy \in I \Rightarrow (x \in I$ or $y \in I)$.

Def. Let R be a unital commutative ring. An ideal I of R is called a prime ideal if

① I is proper, and ② $\forall x, y \in R$, $xy \in I \Rightarrow (x \in I$ or $y \in I)$.

(that means $I \neq R$.)

Theorem. Let R be a unital commutative ring, and $I \triangleleft R$. Then I is a prime ideal if and only if R/I is an integral domain.

(We have already proved it.)

Getting a field as the factor ring is a bit more tricky.

Def. $I \triangleleft R$ is called a maximal ideal if I is proper and $I \subseteq J$ and $J \triangleleft R$ imply either $J = I$ or $J = R$.

We will show that I is maximal ideal $\Leftrightarrow R/I$ is a field.