We have seen that \( \ker \phi \) is an ideal; next we see that kernel of any ring homomorphism is an ideal. In fact we will see

I is an ideal of \( R \) if and only if there is a ring homomorphism \( \phi : R \to R' \) such that

\[
\ker(\phi) = I.
\]

Let’s start by proving \((\Leftarrow)\).

**Lemma.** Suppose \( \phi : R \to R' \) is a ring homomorphism. Then \( \ker \phi \) is an ideal of \( R \).

**Proof.** 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 \( r \in R \).

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

\[
= (\phi(r))(0) = 0.
\]

(Similarly we can show \( \phi(xr) = 0 \); but in this course we are working with commutative rings, and so it is not necessary.)
Next, starting with an ideal $I$ of $R$, we will construct the quotient ring of $R$ by $I$:

**Lemma.** Suppose $I \triangleleft R$. Let $(x+I)(y+I) = xy+I$.

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 subgroup of $G$, then $(g_1N)(g_2N) = g_1g_2N$ 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 $a+N = a'+N \iff a-a' \in N$.

$\begin{align*}
\text{\textit{(\Rightarrow)}} & \ a' \in a+N \Rightarrow a' = a+x \quad \text{for some } x \in N \\
& \Rightarrow a-a' = -x \in N \\
\text{\textit{(\Leftarrow)}} & \ a+N = a' + (a-a') + N = a' + N \\
& \quad \text{as } a-a' \in N \text{ and } N \text{ is a subgroup.}
\end{align*}$

Proof of Lemma.

Well-definedness. $\chi_1 + I = \chi_2 + I \not\Rightarrow \chi_1 y_1 + I = \chi_2 y_2 + I$.

$\begin{align*}
\text{\textit{Proof. From group theory we know that}} & \\
\chi_1 y_1 + I = \chi_2 y_2 + I & \iff \chi_1 y_1 - \chi_2 y_2 \in I; \\
\chi_1 + I = \chi_2 + I & \Rightarrow \chi_1 - \chi_2 \in I \quad \text{\textit{1}} \\
y_1 + I = y_2 + I & \Rightarrow y_1 - y_2 \in I \quad \text{\textit{2}}
\end{align*}$

We have $\chi_1 y_1 - \chi_2 y_2 = \chi_1 y_1 - \chi_2 y_1 + \chi_2 y_1 - \chi_2 y_2$

$\begin{align*}
& = (\chi_1 - \chi_2) y_1 + \chi_2 (y_1 - y_2) \in I \\
& \quad \text{in } I \text{ by \textit{1}} \quad \text{in } I \text{ by \textit{2}}
\end{align*}$
The distributive property and the associativity can be deduced from the fact that $R$ is a ring.

**Lemma.** Suppose $I$ is an ideal of a ring $R$. Then

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

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

(we call $\pi$ the natural quotient map.)

**Proof.** From group theory, we know that $\pi$ is a surjective group homomorphism of $(R, +)$ to $(R/I, +)$; and $\ker \pi = I$.

So it is enough to check that $\pi$ preserves multiplication:

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

and the claim follows.

These lemmas show us that

$I$ is an ideal of $R \iff \exists$ a ring homomorphism $\phi : R \rightarrow R'$

such that $\ker \phi = I$.

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

**Theorem.** Suppose \( \phi : R \rightarrow S \) is a ring homomorphism.

Then

1. \( \text{Im}(\phi) \) is a subring of \( S \) (the image of \( \phi \)).

2. \( \ker(\phi) \) is an ideal of \( R \).

3. \( \bar{\phi} : R/\ker(\phi) \rightarrow \text{Im}(\phi), \bar{\phi}(r + \ker(\phi)) = \phi(r) \) is a ring isomorphism.

**Proof.**

1. Since \( \phi \) is a group homomorphism of \( (R, +) \), \( \text{Im}(\phi) \) is a subgroup of \( (S, +) \). To show it is a subring, it is enough to show it is closed under multiplication:

\[
\forall y_1, y_2 \in \text{Im}(\phi), \exists r_1, r_2 \in R, \ y_1 = \phi(r_1) \text{ and } y_2 = \phi(r_2).
\]

So \( y_1 y_2 = \phi(r_1) \phi(r_2) = \phi(r_1 r_2) \), which implies \( y_1 y_2 \in \text{Im} \phi \).

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 \( (\text{Im}(\phi), +) \). So it is enough to prove \( \bar{\phi} \) preserves multiplication. But
for the sake of completeness, let's recall the group theory part:

**Well-definedness**: \( r_1 + \ker \phi = r_2 + \ker \phi \implies \phi(r_1) = \phi(r_2) \)

\[ r_1 + \ker \phi = r_2 + \ker \phi \implies r_1 - r_2 \in \ker \phi \]

\[ \implies \phi(r_1 - r_2) = 0 \]

\[ \implies \phi(r_1) = \phi(r_2). \]

**Injective**: \( \overline{\phi}(r_1 + \ker \phi) = \overline{\phi}(r_2 + \ker \phi) \implies \phi(r_1) = \phi(r_2) \)

\[ \implies \phi(r_1 - r_2) = 0 \]

\[ \implies r_1 - r_2 \in \ker \phi \implies r_1 + \ker \phi = r_2 + \ker \phi. \]

**Surjective**: \( \forall y \in \text{Im} \phi, \exists r \in \mathbb{R}, y = \phi(r) \)

\[ \implies y = \overline{\phi}(r + \ker \phi). \]

**Preserves addition** is similar to next step. (Do it on your own.)

**Preserves multiplication**: \( \overline{\phi}(r_1 + \ker \phi) \cdot (r_2 + \ker \phi) \)

\[ = \overline{\phi}(r_1 r_2 + \ker \phi) = \phi(r_1 r_2) \]

\[ = \phi(r_1) \phi(r_2) \]

\[ = \overline{\phi}(r_1 + \ker \phi) \overline{\phi}(r_2 + \ker \phi). \]
Ex. Prove that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ as two rings.

**Proof.** Let $c_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the residue homomorphism. Then $c_n(i) = i$ if $0 \leq i < n$. So $\text{Im } c_n = \mathbb{Z}/n\mathbb{Z}$. And $a \in \ker c_n$ if and only if the remainder of $a$ divided by $n$ is $0$.

$$n \mid a \iff a \in n\mathbb{Z}.$$ So by the fundamental homomorphism theorem,

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

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

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

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

**Proof.** (a) 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 $m_{\sqrt{2}}(x) \mid x^2 - 2$. 


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 $\mathbb{Q}$ 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

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

(6) 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

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

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

$$\text{Im} \phi_{\sqrt{2}} \subseteq \mathbb{Q}[\sqrt{2}]. \quad \odot$$

On the other hand, for any $a, b \in \mathbb{Q}$, $\phi_{\sqrt{2}}(a + bx) = a + b\sqrt{2}$; and so $\mathbb{Q}[\sqrt{2}] \subseteq \text{Im} \phi_{\sqrt{2}} \ . \quad \bigodot \odot$ imply the claim.
By the fundamental homomorphism theorem, we have
\[ \mathbb{Q}[x]/\ker \phi_{\sqrt{2}} \cong \mathrm{Im} \phi_{\sqrt{2}}; \text{ and so} \]
\[ \mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}[[\sqrt{2}]]. \]

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

**Proposition.** Suppose \( \alpha \in \mathbb{C} \) is an algebraic number; this means \( \alpha \) is a zero of a polynomial \( f(x) \in \mathbb{Q}[x] \setminus \{0\} \). Let
\[ \phi_{\alpha} : \mathbb{Q}[x] \rightarrow \mathbb{C} \] be the evaluation at \( \alpha \) map; that means
\[ \phi_{\alpha}(f) = f(\alpha). \]

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. \( \mathrm{Im} \phi_{\alpha} = \mathbb{Q}[\alpha] \) is the smallest subring of \( \mathbb{C} \) that contains \( \mathbb{Q} \) as a subset and \( \alpha \) as an element and
   \[ \mathbb{Q}[\alpha] = \{ a_0 + a_1 \alpha + \ldots + a_m \alpha^m | a_i \in \mathbb{Q}, m \in \mathbb{Z}^+ \}. \]
3. \( \mathbb{Q}[x]/m_\alpha(x) \mathbb{Q}[x] \cong \mathbb{Q}[\alpha] \).

**Proof.** Let \( m_\alpha(x) \in \mathbb{Q}[x] \) be the minimal poly. of \( \alpha \) over \( \mathbb{Q} \).
Claim $m_\alpha(x)$ is irreducible.

Proof of claim. 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 $f \in \ker \phi_\alpha = m_\alpha(\alpha)\mathbb{Q}[x]$; this implies $f(x) = m_\alpha(x)q(x)$ 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 $\mathbb{Q}[x]$. 

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

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

\[ \alpha \cdots \alpha = \beta \in A \Rightarrow a_0 \alpha^i \in A \Rightarrow \sum_{i=0}^{m} a_i \alpha^i \in A \]

\[ \Rightarrow \text{Im } \phi_\alpha \subseteq A. \text{ Hence Im } \phi_\alpha \text{ is the smallest subring of } \mathbb{C} \text{ that has } \alpha \text{ as an element and } \emptyset \text{ as a subset.} \]
Consider the ring homomorphism $\phi_a : \mathbb{Q}[x] \to \mathbb{C}$; by the 1st isomorphism theorem

$$\mathbb{Q}[x]/ \ker \phi_a \cong \text{Im} \phi_a ;$$

and so

$$\mathbb{Q}[x]/m_{\phi_a} \cong \mathbb{Q}[x].$$

Next, we would like to show $\mathbb{Q}[x]$ 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 $I \triangleleft \mathbb{R}$ such that $\mathbb{R}/I$ is an integral domain or a field.

We start with the easier case: under what conditions is $\mathbb{R}/I$ an integral domain?

Investigation. Since $R$ is a unital commutative ring,

$R/I$ is an integral domain $\iff$

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

$\iff 1 \ R \neq I. \ \\
\iff 2 \ (x+I)(y+I) = (a+I) \implies \text{either } x+I = a+I \ \\
\quad \quad \quad \quad \text{or } y+I = a+I \ \\
\iff 1 \ I \text{ is a proper ideal } \ 2 \ xy \epsilon I \implies (x\epsilon I \text{ or } y\epsilon I).$

**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. $\forall x, y \in R, \ xy \epsilon I \implies (x \epsilon I \text{ or } y \epsilon I).$

(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 $\iff R/I$ is a field.