# Proper ideals do not have units

Friday, August 25, 2017 12:42 PM

In the previous lecture we defined what an ideal is:

**Def.** Let $R$ be a ring. A non-empty subset $I$ of $R$ is called a ring if ① $\forall x, y \in I$, $x - y \in I$ ($I$ is a subgp of $(R, +)$)

② $\forall r \in R, x \in I$, $rx, xr \in I$.

And we write $I \triangleleft R$.

**Ex.** $\{0\}$ and $R$ are ideals of $R$ for any ring $R$.

**Ex.** Suppose $R$ is a unital ring, $I \triangleleft R$, and $1 \in I$.

Then $I = R$.

**Pf.** Since $1 \in I$ and $I$ is an ideal, for any $r \in R$ we have $r \cdot 1 = r \in I$. So $I = R$. ∎

**Ex.** Suppose $R$ is a unital ring, and $I \triangleleft R$.

If $I \cap U(R) \neq \emptyset$, then $I = R$. (Alternatively we can say: if $I$ is a proper ideal of $R$, then $I \cap U(R) = \emptyset$.)

**Pf.** Suppose $a \in I \cap U(R)$. Then, since $I$ is an ideal and $a \in I$, $(a^{-1})(a) = 1 \in I$. So by the previous example $I = R$. ∎

# Ideals of a field and the ring of integers

Thursday, August 24, 2017 8:57 PM

__Ex.__ Suppose $F$ is a field. Then $I \triangleleft F$ if and only if either $I = \{0\}$ or $I = F$.

__Pf.__ If $I \neq \{0\}$, then $I \cap (F \setminus \{0\}) \neq \emptyset$. Since $U(F) = F \setminus \{0\}$, we get that $I \cap U(F) \neq \emptyset$. Hence by the previous example $I = F$. ∎

__Lemma__. $I \triangleleft \mathbb{Z}$ if and only if $\exists n \in \mathbb{Z}$, $I = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

__Pf.__ ($\Leftarrow$) • $x = nk$, $y = nl \Rightarrow x - y = nk - nl = n\underbrace{(k-l)}_{\in \mathbb{Z}}$

$$\Rightarrow x - y \in n\mathbb{Z}.$$

• $x = nk$, $r \in \mathbb{Z} \Rightarrow rx = xr = n\underbrace{(kr)}_{\in \mathbb{Z}}$

$$\Rightarrow rx, xr \in n\mathbb{Z}.$$

($\Rightarrow$) In fact any subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$, for some $n \in \mathbb{Z}$:

If $I = 0$, then there is nothing to prove.

If $\exists x \in I \setminus \{0\}$, then either $x \in I \cap \mathbb{Z}^+$ or $-x \in I \cap \mathbb{Z}^+$.

So $I \cap \mathbb{Z}^+$ is a non-empty subset of $\mathbb{Z}^+$. Hence by the

# Ideals and principal ideals

Thursday, August 24, 2017 10:56 PM

well-ordering principle $I \cap \mathbb{Z}^+$ has a minimum; let $n = \min I \cap \mathbb{Z}^+$.

Then, as $I$ is subgroup of $(\mathbb{Z}, +)$, we get that $n\mathbb{Z} \subseteq I$.

<u>Claim</u>. $n\mathbb{Z} = I$.

<u>Pf of claim</u>. Suppose $m \in I$. By <u>the division algorithm</u>

$\exists (q,r) \in \mathbb{Z} \times \mathbb{Z}$ s.t. ① $m = nq + r$,

② $0 \leq r < n$.

So $r = m - nq \in I$ as $m, nq \in I$. Since $n$ is the smallest element of $I \cap \mathbb{Z}^+$ and $r < n$, we deduce that $r \notin I \cap \mathbb{Z}^+$. As $r \in I$ and $r \notin I \cap \mathbb{Z}^+$, we get that $r \notin \mathbb{Z}^+$. Because $r \notin \mathbb{Z}^+$ and $0 \leq r < n$, we have $r = 0$; this implies $m = nq \in n\mathbb{Z}$. ∎

<u>Def</u>. Let $R$ be a ring, and $X$ be a non-empty subset of $R$. The smallest ideal of $R$ which contains $X$ is called the ideal generated by $X$; and it is denoted by $\langle X \rangle$. An ideal generated by one element is called a <u>principal ideal</u>.

# Ring of polynomials with coefficients in a field is a PID

Thursday, August 24, 2017 11:14 PM

The previous lemma shows that any ideal of $\mathbb{Z}$ is principal.

<u>Def.</u> An integral domain $D$ is called a

Principal Ideal Domain (PID) if any ideal is principal.

<u>Ex.</u> $\mathbb{Z}$ is a PID.

<u>Theorem.</u> Let $F$ be a field. Then $F[x]$ is a PID.

(Its proof is fairly similar to the previous proof, and it is based on the division algorithm in $F[x]$. This method can be applied for other rings as well.)

<u>Proof.</u> Let $I \triangleleft F[x]$. If $I = \{0\}$, there is nothing to prove. If not, let $f_0(x) \in I$ be such that

$$\deg f_0 = \min\{\deg g \mid g \in I, g \neq 0\}.$$

(By the well-ordering principle there is such a polynomial $f_0$).

<u>Claim.</u> $I = \langle f_0 \rangle$.

<u>Pf of claim.</u> Suppose $g(x) \in I$. Then by <u>the division algorithm</u> there are $q, r \in F[x]$ such that

# F[x] is a PID.

Thursday, August 24, 2017 11:32 PM

① $g(x) = f_0(x)\, q(x) + r(x)$,

② $\deg r < \deg f_0$.

Since $f_0(x) \in I$ and $I$ is an ideal, we have $f_0(x) q(x) \in I$.

As $g(x) \in I$ and $f_0(x) q(x) \in I$, we get that

$$r(x) = g(x) - f_0(x)\, q(x) \in I.$$

Since $\deg f_0 = \min\{\deg f \mid f \in I, f \neq 0\}$, $\deg r < \deg f_0$,

and $r \in I$, we deduce that $r = 0$; this implies

$$g(x) = f_0(x)\, q(x) \in \langle f_0(x) \rangle. \quad \blacksquare$$

We quickly defined the ideal generated by a non-empty subset $X$, and we did not justify our definition:

<u>Lemma</u>. Let $\{I_a \mid a \in A\}$ be a family of ideals of a ring $R$. Then $\bigcap_{a \in A} I_a$ is an ideal of $R$. In particular for a non-empty subset $X$ of $R$, $\bigcap_{\substack{I \trianglelefteq R \\ X \subseteq I}} I$ is an ideal of $R$ and $\langle X \rangle = \bigcap_{\substack{I \trianglelefteq R \\ X \subseteq I}} I$.

<u>Pf.</u> $x, y \in \bigcap_{a \in A} I_a \Rightarrow \forall a \in A,\ x, y \in I_a \Rightarrow \forall a \in A,\ x - y \in I_a$

# Elements of a principal ideal

Thursday, August 24, 2017 11:44 PM

So $x-y \in \bigcap_{a\in A} I_a$.

- Suppose $x \in \bigcap_{a\in A} I_a$ and $r\in R$. Then, for any $a\in A$, we have $x\in I_a$. Since $I_a$ is an ideal, $x\in I_a$, and $r\in R$, we get $rx, xr \in I_a$ (for any $a\in A$). Hence

$$rx, xr \in \bigcap_{a\in A} I_a.$$

- Let $J := \bigcap_{\substack{I\triangleleft R\\ X\subseteq I}} I$. Then, by the first part, $J \triangleleft R$; and clearly $X \subseteq J$.

Now, if $X\subseteq I'$ and $I'\triangleleft R$, then $I' \supseteq \bigcap_{\substack{I\triangleleft R\\ X\subseteq I}} I = J$.

So $J$ is the smallest ideal which contains $X$. ■

<u>Lemma</u>. Let $R$ be a commutative unital ring. For $a\in R$, we have $\langle a\rangle = aR = \{ar \mid r\in R\}$.

<u>Pf</u>. ($\supseteq$) Since $a\in\langle a\rangle$, for any $r\in R$ we have $ar\in\langle a\rangle$.

So $\langle a\rangle \supseteq aR$.

($\subseteq$) Since $R$ is unital, $a\in aR$. So using the previous lemma, it is enough to show $aR$ is an ideal.

# Ideals and the kernels of ring homomorphisms

Thursday, August 24, 2017 11:57 PM

- $\forall\, r_1, r_2 \in R$, $ar_1 - ar_2 = a\underbrace{(r_1 - r_2)}_{\text{in } R}$. So $ar_1 - ar_2 \in aR$.

- $\forall\, r, r' \in R$, $r(ar') = (ar')r = a\underbrace{(r'r)}_{\text{in } R}$.

  So $r(ar'), (ar')r \in aR$. ■

<u>Why should we care about ideals?</u>

Next we will see that

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

We will show this in many steps and along the way we will define <u>the quotient ring of $R$ by $I$</u>.

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>. Since $\phi$ is an additive group homomorphism, $\ker\phi$ is a subgroup of $(R, +)$. Now suppose $x \in \ker\phi$ and $r \in R$.

# The quotient ring

Friday, August 25, 2017 12:10 AM

$\phi$ is a ring homomorphism

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

$x \in \ker\phi$

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

this implies $rx \in \ker\phi$. Similarly we have

$\phi(xr) = \phi(x)\phi(r) = (0)(\phi(r)) = 0$; and so

$xr \in \ker\phi$.

Therefore $\ker\phi$ is an ideal of $R$. ∎

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

<u>Lemma</u>. 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 $g \in G$, $gN = Ng$.

# The quotient ring

Friday, August 25, 2017 12:23 AM

In group theory, you have seen that, if $N$ is a normal subgp of $G$, then $(g_1N)\cdot(g_2N) = g_1g_2N$ 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 if $I$ is an ideal of $R$.

Proof of Lemma.

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

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 $\quad x_1y_1 - x_2y_2 = x_1y_1 - x_2y_1 + x_2y_1 - x_2y_2$

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

# 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 $\pi$ the <u>natural quotient map</u>.)

<u>Pf.</u> 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:

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

and the claim follows. ■

These lemmas show us that

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