Lecture 12: Kernel of an evaluation map

Saturday, February 23, 2019 5:00 PM

Suppose $\alpha \in \mathbb{C}$ is an algebraic number; that means α is a zero of a polynomial $p(x) \in \mathbb{Q}[x] \setminus \{0\}$. Let $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation at α. Then $\ker \phi_\alpha = \{ f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0 \}$. Here are two basic properties of $\underline{\ker \phi_\alpha}$:

(a) $f_1, f_2 \in \ker \phi_\alpha \Rightarrow f_1 + f_2 \in \ker \phi_\alpha$

$$f_1(\alpha) = f_2(\alpha) = 0 \Rightarrow f_1(\alpha) + f_2(\alpha) = 0$$

(b) $f \in \ker \phi_\alpha$, $g \in \mathbb{Q}[x] \Rightarrow g(x) \cdot f(x) \in \ker \phi_\alpha$.

$$f(\alpha) = 0 \Rightarrow g(\alpha) \cdot f(\alpha) = (g(\alpha))(0) = 0$$

Next we consider a subset of a unital commutative ring A with the above properties:

<u>Def</u>. Let A be a unital commutative ring; $I \subseteq A$ is called an <u>ideal</u> if ① $\forall x, y \in I$, $x - y \in I$ (additive subgp)

② $\forall a \in A$, $x \in I$, $ax \in I$.

We write $I \triangleleft A$. (or $I \trianglelefteq A$.)

Lecture 12: A historical note on ideals

Wednesday, August 23, 2017 11:53 PM

<u>A historical note</u>. In order to solve Fermat's last conjecture, which says the only integer solutions of $x^n+y^n=z^n$ are the trivial ones if $n\geq 3$, Kummer studied rings of the form $\mathbb{Z}[\zeta_n]$ where ζ_n is an n^{th} root of unity. In such rings an element does not necessarily of <u>unique</u> factorization into "prime" factors; but Kummer showed in appropriate sense <u>ideals</u> do have such a unique factorization; and he called them <u>ideal numbers</u>. Later Dedekind, Hilbert, and Noether developed the theory of ideals for general rings.

(In one of the exercises you are working with $\mathbb{Z}[\omega]$, where ω is a 3^{rd} root of unity.)

<u>Ex.</u> $\{0\}$ and R are ideals of R for any ring R.

<u>Ex.</u> Suppose R is a unital ring, $I \triangleleft R$, and $1\in I$. Then $I=R$.

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

Lecture 12: Proper ideals do not have units

Friday, August 25, 2017 12:42 PM

__Ex.__ Suppose R is a unital ring, and $I \triangleleft R$.

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

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

__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 $F^\times = F \setminus \{0\}$ we get that $I \cap F^\times \neq \emptyset$. 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.__ ($\Leftarrow$). • $x = nk$, $y = nl \Rightarrow x - y = nk - nl = n\underbrace{(k-l)}_{\in \mathbb{Z}}$

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

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

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

Lecture 12: Ideals of the ring of integers

Thursday, August 24, 2017 8:57 PM

($\Leftarrow$) 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 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) $0\le r<n$.

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 $0\le r<n$, we have $r=0$; this

Lecture 12: Ideals and principal ideals

Thursday, August 24, 2017 10:56 PM

implies $m = nq \in n\mathbb{Z}$. ∎

Def.\Lemma. Suppose A is a unital commutative ring. Then for any $a \in A$ the set aA of all multiples of a is an ideal of A. This type of ideal is called a principal ideal.

Pf. $\cdot\ b_1, b_2 \in aA \Rightarrow \exists\, a_1, a_2 \in A,\ b_1 = aa_1,\ b_2 = aa_2$

$$\Rightarrow b_1 + b_2 = aa_1 + aa_2 = a(a_1 + a_2) \in aA$$

$\cdot\ b \in aA \Rightarrow \exists\, a' \in A,\ b = aa'$

$$\Rightarrow \forall a'' \in A,\ a'' b = a''(aa')$$

$$= a(a''a') \in aA. \ ∎$$

We have seen that any ideal of $\mathbb{Z}$ is principal.

Def. An integral domain D is called a Principal Ideal Domain (PID) if any ideal is principal.

Ex. $\mathbb{Z}$ is a PID.

Lecture 12: F[x] is a PID

Thursday, August 24, 2017 11:14 PM

Theorem. 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.)

Proof. 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).

Claim. $I = f_0(x)\,F[x]$.

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

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 $f_0(x)q(x) \in I$.

Lecture 12: F[x] is a PID.

Thursday, August 24, 2017 11:32 PM

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

$$g(x) = f_0(x)\, q(x) \in f_0(x) F[x]. \qquad \blacksquare$$

Going back to <u>ker</u> ϕ_α where $\alpha \in \mathbb{C}$ is an algebraic number, we have that $\ker \phi_\alpha \triangleleft \mathbb{Q}[x]$. Using the previous theorem we deduce:

<u>Lemma</u>. Suppose $\alpha \in \mathbb{C}$ is an algebraic number. Then there is a unique monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ such that $\ker \phi_\alpha = m_\alpha(x)\mathbb{Q}[x]$; this means α is a zero of a polynomial $f(x) \in \mathbb{Q}[x]$ if and only if $m_\alpha(x) \mid f(x)$. In particular $m_\alpha(x)$ has smallest degree among non-zero polynomials in $\mathbb{Q}[x]$ that have α as a zero. $m_\alpha(x)$ is called the minimal polynomial of α over $\mathbb{Q}$.

Lecture 12: Minimal polynomial

Saturday, February 23, 2019 8:33 PM

Pf. $\left.\begin{array}{l}\ker \phi_\alpha \lhd \mathbb{Q}[x] \\ \mathbb{Q}[x] \text{ is a PID}\end{array}\right\} \Rightarrow \exists\, m_\alpha(x) \in \mathbb{Q}[x]$ s.t. $\ker \phi_\alpha = m_\alpha(x)\, \mathbb{Q}[x]$.

Since α is algebraic, $\exists\, f(x) \in \mathbb{Q}[x] \setminus \{0\}$, $f(\alpha) = 0$; and so $\ker \phi_\alpha \neq 0$. Hence $m_\alpha(x) \neq 0$. So after multiplying by the inverse of the leading coefficient of $m_\alpha(x)$, we can and will assume $m_\alpha(x)$ is a monic polynomial.

Uniqueness. Suppose $m_1(x)\, \mathbb{Q}[x] = m_2(x)\, \mathbb{Q}[x]$ for two monic polynomials. Then $m_1(x) = m_2(x)\, q(x)$ and $m_2(x) = m_1(x)\, q'(x)$; and so $m_1(x) = m_1(x)\, q(x)\, q'(x)$. Hence $q_1 \cdot q'_1 = 1$, which implies $q_1 \in \mathbb{Q}[x]^\times = \mathbb{Q}^\times$. Thus $m_1(x) = q_1\, m_2(x)$ implies the leading coeff of m_1 is q_1 times the leading coeff. of m_2. As m_1 and m_2 are monic, we deduce $q_1 = 1$ and $m_1(x) = m_2(x)$.

The rest of claims are clear. ∎