3/18/14

Welcome Back!

HW 3 due this Thursday

NO CLASS NEXT TUESDAY (Sorry).

HW 4 due Tues Apr 1.

Exam 2 Thurs Apr 3.

---

Q: What do $\mathbb{Z}$ and $K[x]$ have in common?

A: They are both PIDs (Principal Ideal Domains).

Let $R$ be a ring. Given $a \in R$ we consider the principal ideal

$$(a) = aR := \{ar : r \in R\}.$$

We have $(1) = R$. Furthermore,

$$(a) = (1) \iff a \in R^\times$$
(a is a unit).

Given $a, b \in R$ we say "b divides a" and write $b \mid a$ if

$$\exists\, r \in R \text{ such that } a = br.$$

Note that

$$(a) \leq (b) \iff b \mid a.$$

Now let $R$ be a <u>domain</u>. Then we have

$$(a) = (b) \iff a, b \text{ are } \underline{\text{associate}},$$
i.e., $\exists\, u \in R^{\times}$ with $a = bu$.

<u>Proof</u>: If $\exists\, u \in R^{\times}$ with $a = bu$ then

$$a = bu \implies a \in (b) \implies (a) \leq (b)$$
$$b = au^{-1} \implies b \in (a) \implies (b) \leq (a).$$

Hence $(a) = (b)$. Conversely, if $(a) = (b)$ then

$$a \in (b) \implies a = br \text{ for some } r \in R.$$
$$b \in (a) \implies b = as \text{ for some } s \in R.$$

Then
$$a = br$$
$$a = asr$$
$$a(1 - rs) = 0$$

If $a=0$ there is nothing to show. If $a\neq 0$ then since $R$ is a domain we have

$$1-rs=0$$
$$1=rs,$$

i.e., $r,s\in R^\times$. We conclude that $a,b$ are associate. ///

[ Recall that

$$\mathbb{Z}^\times=\{\pm 1\} \quad \& \quad K[x]^\times = K^\times = K-\{0\}.$$

Thus for $m,n\in\mathbb{Z}$ we have

$$(m)=(n) \iff m=\pm n$$

and for $f(x),g(x)\in K[x]$ we have

$$(f(x))=(g(x)) \iff f(x)=\alpha g(x) \text{ for some } 0\neq\alpha\in K.$$ ]

Q: What does

$$(a)\underset{\neq}{<}(b)\underset{\neq}{<}(1) \quad \text{mean?}$$

We have

- $b \mid a$
- $b$ not associate to $a$
- $b$ not a unit.

In this case we say $b$ is a *proper divisor* of $a$.

*Definition*: We say $a \in R$ is *irreducible* if it has NO PROPER DIVISORS.

☆ *Theorem*: If $R$ is a PID then every element can be written as a product of irreducibles, times a unit.

[Recall the Proof for $\mathbb{Z}$: Consider $n \in \mathbb{Z}$. If $n$ is irreducible or a unit, we're done. So assume we can write

$$n = a_1 b_1$$

with $1 < |a_1|, |b_1| < |n|$. If $a_1, b_1$ are irreducible we're done. So assume WLOG that $a_1$ is reducible:

$$a_1 = a_2 b_2$$

with $1 < |a_2|, |b_2| < |a_1|$. Assume for contradiction that $n$ has no irreducible factorization. Then we obtain an infinite sequence

$$|n| > |a_1| > |a_2| > |a_3| > \cdots > 1.$$

This contradicts the well-ordering property of $\mathbb{N}$. /// ]

In a general PID we can't use well-ordering. We need a new idea.

<u>Lemma</u>: Let $R$ be a PID. Then $R$ does NOT contain an infinite strictly increasing sequence of ideals

$$J_1 < J_2 < J_3 < \cdots$$

<u>Proof</u>: Assume for contradiction that such an infinite chain exists, and let

$$J := \bigcup_{i=1}^{\infty} J_i .$$

I claim that $J$ is an ideal. Indeed, given any $a, b \in J$, $\exists\ m, n \in \mathbb{N}$ such that

$$a \in J_m \quad \& \quad b \in J_n$$

Then $a, b \in J_{\max\{m,n\}}$ and hence $a - b \in J_{\max\{m,n\}} \subseteq J$. Thus $(J, +, 0)$ is a subgroup of $(R, +, 0)$.

Next, given any $a \in J$ and $r \in R$, $\exists$ $m \in \mathbb{N}$ such that $a \in J_m$. Since $J_m$ is an ideal we have

$$ar \in J_m \subseteq J.$$

Hence $J$ is an ideal.

Finally, since $R$ is a PID we have $J = (c)$ for some $c \in R$. Since $c \in J$ there exists $N \in \mathbb{N}$ such that $c \in J_N$. But then

$$J = (c) \subseteq J_N < J_{N+1} \subseteq J.$$

Contradiction. $\blacksquare$

Jargon: We say that a ring $R$ is Noetherian if it has no infinite increasing chain of ideals. We just proved that

$$\text{PID} \Longrightarrow \text{Noetherian}.$$

"Noetherian" is the abstract version of well-ordering. ///

Now we can prove the theorem ☆.

Proof: Let $R$ be a PID and consider any nonzero nonunit $a \in R$. Assume for contradiction that $a$ can not be expressed as a product of irreducibles, times a unit.

Then $a$ is not itself irreducible, so we have

$$a = a_1 b_1$$

with $(a) < (a_1), (b_1) < (1)$.

Now $a_1, b_1$ are <u>not</u> <u>both</u> irreducible. WLOG say $a_1$ is not irreducible. Then

$$a_1 = a_2 b_2$$

with $(a_1) < (a_2), (b_2) < (1)$. Continuing in this way we obtain an infinite chain of ideals

$$(a) < (a_1) < (a_2) < \cdots,$$

contradicting the fact that $R$ is Noetherian.

$\blacksquare$.

Thus every $a \in R$ in a PID can be factored as

$$a = u p_1 p_2 \cdots p_k$$

where $u \in R^\times$ and $p_1, \ldots, p_k$ are irreducible.

Q: Is the factorization unique?

A: How did we prove uniqueness for $\mathbb{Z}$?

Recall Euclid's Lemma:

If $p \in \mathbb{Z}$ has factors $\pm 1$ and $\pm p$ then for all $a, b \in \mathbb{Z}$ we have

$$p \mid ab \implies p \mid a \text{ OR } p \mid b.$$

Proof: Assume that $p \mid ab$ (say $ab = pk$) and $p \nmid a$. Then $\gcd(a,p) = 1$ so there exist $x, y \in \mathbb{Z}$ with

$$ax + py = 1.$$

Multiply by $b$ to get

$$\begin{aligned} abx + pby &= b \\ pkx + pby &= b \\ p(kx + by) &= b. \end{aligned}$$

$\implies p \mid b$. ///

Then we prove unique factorization:
Given $n \in \mathbb{Z}$ assume we have

$$n = \pm p_1 p_2 \cdots p_k = \pm q_1 q_2 \cdots q_\ell$$

with $p_i$ and $q_j$ irreducible. Then

$$p_1 \mid n$$
$$p_1 \mid q_1 q_2 \cdots q_\ell$$

$\Longrightarrow p_1 \mid q_j$ for some $j$ (by Euclid).

WLOG say $p_1 \mid q_1$. Since $q_1$ is irreducible this implies $p_1 = \pm q_1$. Since $R$ is a domain we can <u>cancel</u> to get

$$\pm p_2 p_3 \cdots p_k = \pm q_2 q_3 \cdots q_\ell.$$

Continuing in this way we get $k = \ell$ and

$$\begin{aligned} p_2 &= \pm q_2 \\ p_3 &= \pm q_3 \\ &\vdots \\ p_k &= \pm q_k. \end{aligned}$$

$\blacksquare$

3/20/14

HW 3 due NOW
HW 4 due Tues Apr 1
Exam 2 Thurs Apr 3
NO CLASS NEXT Tues Mar 25

Recall: We are developing the theory of Principal Ideal Domains (PIDs).

Let $R$ be a PID, i.e., every ideal $I \subseteq R$ is generated by a single element:

$I = (a) = \{ar : r \in R\}$ for some $a \in R$.

Last time we proved

Lemma: PIDs are Noetherian.

That is, if $R$ is a PID then there does NOT exist an infinite increasing chain of ideals

$$J_1 < J_2 < J_3 < \cdots$$

Proof: Show that $J := \bigcup_{i=1}^{\infty} J_i$ is an ideal.

Since $R$ is a PID this implies $J=(a)$. Since $a \in J$ we have $a \in J_n$ for some $n$. But then

$$J=(a) \leq J_n \underset{\neq}{<} J_{n+1} \leq J.$$

Contradiction //

We can use the Noetherian property like the well-ordering principle to prove

<u>Theorem</u>: Every $a \in R$ in a PID can be written as a product of irreducibles times a unit.

<u>Proof</u>: If $a$ is irreducible we're done. Otherwise we have

$$a = a_1 b_1$$

for some $(a) < (a_1), (b_1) < (1)$. If $a_1$ and $b_1$ are irreducible we're done. Otherwise WLOG we have

$$a_1 = a_2 b_2$$

for some $(a_1) < (a_2), (b_2) < (1)$.

If $a$ has no factorization then we obtain an infinite chain

$$(a) < (a_1) < (a_2) < \cdots$$

contradicting the fact that $R$ is Noetherian. We conclude that $a$ has a factorization. //

Thus every $a \in R$ in a PID $R$ can be expressed as

$$a = u p_1 p_2 \cdots p_k$$

with $u \in R^\times$ and $p_1, p_2, \ldots, p_k \in R$ irreducible.

[Recall: We say $p \in R$ is irreducible if

$$p = ab \implies a \text{ or } b \text{ is a unit.}$$ ]

Q: Is the expression $a = u p_1 \cdots p_k$ UNIQUE?

A: How did we prove uniqueness for $\mathbb{Z}$?
We used

Euclid's Lemma: If $p \in \mathbb{Z}$ is <u>irreducible</u>,

i.e., $p = ab \implies a = \pm 1$ or $b = \pm 1$

then $p$ is <u>prime</u>,

i.e., $p \mid ab \implies p \mid a$ or $p \mid b$.

<u>Proof</u>: Let $p \in \mathbb{Z}$ be irreducible and suppose that $p \mid ab$ with $p \nmid a$.
We will show that $p \mid b$.

First let $d = \gcd(a, p)$. Since $d \mid p$ and $p$ is irreducible we have $d = 1$ or $d = p$. Then since $d \mid a$ and $p \nmid a$ we have $d = 1$. By Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that

$$ax + py = 1.$$

(So what?)

Now multiply by $b$ and use the fact that $p \mid ab$ (say $ab = pk$) to get

$$\begin{aligned} ax + py &= 1 \\ abx + pby &= b \\ pkx + pby &= b \\ p(kx + by) &= b. \end{aligned}$$

We conclude that $p \mid b$. ///

Now we can prove unique factorization. Given $n \in \mathbb{Z}$ suppose we have

$$n = \pm p_1 p_2 \cdots p_k = \pm q_1 q_2 \cdots q_l$$

with the $p_i$ and $q_j$ irreducible. Then

$$\begin{aligned} &p_1 \mid n \\ &p_1 \mid q_1 q_2 \cdots q_l. \end{aligned}$$

Euclid's Lemma then implies that

$$p_1 \mid q_j \quad \text{for some } j.$$

WLOG suppose that $p_1 \mid q_1$. Since $q_1$ is irreducible and $p_1 \neq \pm 1$ we have

$$p_1 = \pm q_1$$

Since $\mathbb{Z}$ is a domain we can cancel to get

$$\pm p_2 p_3 \cdots p_k = \pm q_2 q_3 \cdots q_\ell .$$

Continuing in this way we get $k = \ell$ and

$$\begin{aligned} p_2 &= \pm q_2 \\ p_3 &= \pm q_3 \\ &\vdots \\ p_k &= \pm q_k \end{aligned}$$

$\blacksquare$

We will show that the same proof works over a PID. But first some definitions.

$\downarrow$

Definitions: Let $R$ be a ring.

- We say that $p \in R$ is irreducible if

$$p = ab \implies a \text{ or } b \text{ is a unit.}$$

- We say that $p \in R$ is prime if

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Proposition: If $R$ is a domain then

$$p \in R \text{ prime} \implies p \in R \text{ irreducible}.$$

Proof: Suppose that $p \in R$ is prime and let $p = ab$. Then since $p \mid ab$ (indeed, $ab = 1p$) we have

$$p \mid a \quad \text{or} \quad p \mid b.$$

WLOG suppose $p \mid a$, say $a = pk$. Then we have

$$p = ab = pkb$$
$$p - pkb = 1$$
$$p(1 - kb) = 1.$$

If $p \neq 0$ then since $R$ is a domain we have

$$1 - kb = 0$$
$$1 = kb.$$

$\Longrightarrow$ $b$ is a unit.
Hence $p$ is irreducible. ///

But the converse is not true in all domains.

<u>Example</u>: Consider the ring

$$\mathbb{Z}[\sqrt{-3}] := \{ a + b\sqrt{-3} : a, b \in \mathbb{Z} \}$$

You will show on HW4 that $\mathbb{Z}[\sqrt{-3}]$ is a domain. However, the element

$$2 \in \mathbb{Z}[\sqrt{-3}]$$

is irreducible but NOT prime. ///

This does not happen in a PID.

Theorem (Euclid's Lemma for PIDs):

Let $R$ be a PID. Then

$$p \in R \text{ irreducible} \Longrightarrow p \in R \text{ prime}.$$

Proof: Let $p$ be irreducible. Suppose that $p \mid ab$ (say $ab = pk$) but $p \nmid a$. We will show that $p \mid b$.

Since $a \notin (p)$ we have a strict inclusion of ideals

$$(p) < (p) + (a)$$

Since $R$ is a PID we have $(p) + (a) = (d)$ for some $d \in R$, hence

$$(p) < (d) \leq (1).$$

Then since $p$ is irreducible we have $(d) = (1)$.

We conclude that

$$(p) + (a) = (1)$$

(the ideals are coprime).

Thus $\exists\, x, y \in R$ such that

$$px + ay = 1$$
$$pbx + aby = b$$
$$pbx + pky = b$$
$$p(bx + ky) = b.$$

We conclude that $p \mid b$ as desired. ///

Finally, we have an important

Theorem: PID $\Longrightarrow$ UFD.

That is, every nonzero, nonunit element of a PID can be expressed uniquely as a product of irreducible elements times a unit

Proof: Existence of factorization follows from the fact that

$$\text{PID} \Rightarrow \text{Noetherian}.$$

Then the uniqueness of factorization follows from the fact that

$$p \in R \text{ irreducible} \Rightarrow p \in R \text{ prime}$$

"Euclid's Lemma". $\blacksquare$

3/27/14

HW 4 due next Tues Apr 1.
Exam 2 next Thurs Apr 3

Where are we?
We finished a nice piece of abstract ring theory:

$$\text{Euclidean} \Longrightarrow \text{PID} \Longrightarrow \text{UFD}$$

This involved putting the old theory of $\mathbb{Z}$ into the elegant language of PIDs.

Next we will apply our knowledge to the other famous kind of PID (i.e. $K[x]$).
In summary, we have

1. Study of $\mathbb{Z}$
2. Study of PIDs
3. Study of $K[x]$

For the rest of the course we will discuss (3), with the goal of <u>solving</u> polynomial equations

$$f(x) = 0.$$

So let $K$ be a field and consider any field $L \supseteq K$ containing $K$ as a subring, i.e.,

- $(K, +, 0)$ is a subgroup of $(L, +, 0)$
- $(K^\times, \times, 1)$ is a subgroup of $(K^\times, \times, 1)$

[Example: $\mathbb{R} \supseteq \mathbb{Q}$].

For short we will call $L \supseteq K$ a field extension.

Now suppose we have a ring homomorphism

$$\varphi : K[x] \to L$$

with the property that $\varphi|_K : K \to L$ is the identity, i.e., for all $k \in K \subseteq K[x]$ we have

$$\varphi(k) = k \in K \subseteq L.$$

How does $\varphi$ act on a general polynomial

$$f(x) = \sum_k a_k x^k \quad K[x] \; ?$$

Since $\varphi$ is a homomorphism we have

$$\varphi\left(\sum_k a_k x^k\right) = \sum_k \varphi\left(a_k x^k\right)$$
$$= \sum_k \varphi(a_k)\,\varphi(x)^k$$
$$= \sum_k a_k\,\varphi(x)^k.$$

So the map is completely determined once we choose the value $\varphi(x) \in L$.

Let $\alpha := \varphi(x) \in L$. Then we have

$$\varphi\left(\sum_k a_k x^k\right) = \sum_k a_k \alpha^k.$$

We will call this map "evaluation at $\alpha$"

$$ev_\alpha : K[x] \longrightarrow L$$

and for simplicity we will write

$$f(\alpha) := ev_\alpha\left(f(x)\right) \in L.$$

We have a special notation for the image:

$$K[\alpha] := \mathrm{im}(ev_\alpha) \subseteq L.$$

$$= \{ f(\alpha) : f(x) \in K[x] \}$$

$$= \{ \sum_k a_k \alpha^k : a_k \in K \ \forall k \}.$$

$$= \text{"}K \text{ adjoin } \alpha\text{"}$$

This is the smallest subring of $L$ that contains $K$ and $\alpha$ (i.e. the subring of $L$ "generated" by $K$ and $\alpha$).

What about the kernel?

Since $K[x]$ is a PID we know that

$$\ker(ev_\alpha) = (m_\alpha(x))$$

for some polynomial $m_\alpha(x) \in K[x]$.
Recall that

$$(f(x)) = (m_\alpha(x))$$

$$\Updownarrow$$

$$f(x) = \lambda m_\alpha(x) \text{ for some } \lambda \in K^\times$$

So we can assume that $m_\alpha(x)$ has leading coefficient $= 1$. This $m_\alpha(x)$ is called

the minimal polynomial of $\alpha \in L$ over $K$.

Example: Consider the evaluation of $\mathbb{R}[x]$ at the complex number $i \in \mathbb{C}$.

$$ev_i : \mathbb{R}[x] \longrightarrow \mathbb{C}$$
$$f(x) \longmapsto f(i).$$

On HW 2 you showed that the minimal polynomial of $i$ over $\mathbb{R}$ is

$$m_i(x) = x^2 + 1 \in \mathbb{R}[x].$$

Q: What is the minpoly. of $i$ over $\mathbb{C}$?

$$ev_i : \mathbb{C}[x] \longrightarrow \mathbb{C}$$
$$f(x) \longmapsto f(i)$$

has kernel $(m_i(x)) = (x - i)$
$= \{(x-i)f(x) : f(x) \in \mathbb{C}[x]\}$

☆ Descartes' Factor Theorem (1637):

Let $K$ be a field and consider any $\alpha \in K$. Then the evaluation map

$$\begin{aligned} ev_\alpha : K[x] &\to K \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

has kernel

$$\ker(ev_\alpha) = \{(x-\alpha)f(x) : f(x) \in K[x]\}.$$

In other words, the minimal polynomial of $\alpha \in K$ over $K$ is

$$m_\alpha(x) = x - \alpha \in K[x].$$

////

Proof: Given $f(x) \in K[x]$ and $\alpha \in K$ we want to show that

$$f(\alpha) = 0 \iff (x-\alpha) \mid f(x) \text{ in } K[x].$$

First suppose that $(x-\alpha) \mid f(x)$, i.e.,

$$f(x) = (x-\alpha)g(x) \text{ with } g(x) \in K[x].$$

Then evaluate at $\alpha$ to get

$$\begin{aligned} f(\alpha) &= (\alpha-\alpha)g(\alpha) \\ &= 0 \cdot g(\alpha) \\ &= 0. \end{aligned}$$

Conversely, suppose that $f(\alpha) = 0$. By the Division Algorithm there exist $q(x), r(x) \in K[x]$ such that

- $f(x) = q(x)(x-\alpha) + r(x)$
- $r(x) = 0$ or $\deg(r) < \deg(x-\alpha) = 1$

We conclude that $r(x) = r \in K$ is a constant. Then evaluating at $\alpha$ gives

$$\begin{aligned} f(\alpha) &= q(\alpha)(\alpha-\alpha) + r \\ 0 &= q(\alpha) \cdot 0 + r \\ 0 &= r. \end{aligned}$$

Hence $f(x) = q(x)(x-\alpha)$ as desired.

$\blacksquare$

How do we know that $x^2+1 \in \mathbb{R}[x]$ is the minpoly for $i \in \mathbb{C}$ over $\mathbb{R}$ ?

Proof: Let $m_i(x) \in \mathbb{R}[x]$ be the minpoly for $i \in \mathbb{C}$ over $\mathbb{R}$, i.e., let

$$\ker(ev_i) = \{ f(x) \in \mathbb{R}[x] : f(i) = 0 \} = \{ m_i(x) g(x) : g(x) \in \mathbb{R}[x] \}.$$

Since $x^2+1 \in \ker(ev_i)$ we have

$$x^2+1 = m_i(x) g(x)$$

for some $g(x) \in \mathbb{R}[x]$. I claim that we must have $g(x) = 1$.

Since $i \notin \mathbb{R}$ we know that $\deg(m_i) \geq 2$ [If $\deg(m_i) = 1$ and $m_i(i) = 0$ then we must have $m_i(x) = x - i$, which is not in $\mathbb{R}[x]$. If $\deg(m_i) = 0$ and $m_i(i) = 0$ then we must have $m_i(x) = 0$, which implies $x^2+1 = 0$. Contradiction.]

Applying degrees gives

$$\begin{aligned} 2 &= \deg(x^2+1) \\ &= \deg(m_i(x)\,g(x)) \\ &= \deg(m_i) + \deg(g) \\ &= 2 + \deg(g) \end{aligned}$$

$\implies \deg(g) = 0$

$\implies g(x)$ is a constant.

Then since $m_i(x)$ has leading coefficient $= 1$ and

$$x^2 + 1 = m_i(x)\, g(x)$$

we conclude that $g(x) = 1$. Hence

$$m_i(x) = x^2 + 1.$$

//

Q: What is the minimal polynomial for $\pi = 3.14\ldots \in \mathbb{R}$ over $\mathbb{Q}$?

A: Consider the evaluation map

$$\begin{aligned} ev_\pi : \mathbb{Q}(x) &\longrightarrow \mathbb{R} \\ f(x) &\longmapsto f(\pi). \end{aligned}$$

In 1882, Lindemann proved that the kernel is

$$\ker(ev_\pi) = (0).$$

Hence the minimal polynomial is

$$m_\pi(x) = 0 \in \mathbb{Q}[x].$$

Notation: Given $\alpha \in L \supseteq K$ we say that

"$\alpha$ is algebraic over $K$"

if $\ker(ev_\alpha) \neq (0)$ (i.e. if $\deg(m_\alpha) \geq 1$).
If $\ker(ev_\alpha) = (0)$ (i.e. if $m_\alpha(x) = 0$)
we say that

"$\alpha$ is transcendental over $K$".

Example:

- $\sqrt{2}$ is algebraic over $\mathbb{Q}$
- $\pi$ is transcendental over $\mathbb{Q}$
- $i$ is algebraic over $\mathbb{R}$
- $\pi$ is algebraic over $\mathbb{R}$.

Given $\alpha \in L \supseteq K$ the First Isomorphism Theorem says that

$$\frac{K[x]}{(m_\alpha(x))} = \frac{K[x]}{\ker(ev_\alpha)} \approx im(ev_\alpha) = K[\alpha]$$

$$\Longrightarrow \boxed{K[\alpha] \approx K[x]/(m_\alpha(x)).}$$

<u>Example</u>:

$$\mathbb{C} = \mathbb{R}[i] \simeq \mathbb{R}[x]/(x^2+1).$$

---

But $\mathbb{C}$ is not just a ring.
We can also <u>divide</u>

$$\frac{1}{a+bi} = \frac{1}{a+bi}\frac{(a-bi)}{(a-bi)}$$

$$= \frac{a-bi}{a^2+b^2}$$

$$= \left(\frac{a}{a^2+b^2}\right) + \left(\frac{-b}{a^2+b^2}\right) i$$

What does this mean?