2/3/14

HW 1 due NOW
I will hand out HW 2 on Thurs

Recall: Last time we proved that for all $m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$ we have

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\approx} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

↑ ring isomorphism.

To do this we defined

$$\varphi([a]_{mn}) := ([a]_m, [a]_n)$$

and showed that φ is a bijection that preserves ring structure. The hardest part was to show that φ is surjective. For this we use the Euclidean algorithm to find (non-unique!) $x, y \in \mathbb{Z}$ such that

$$1 = mx + ny$$

Then we have

$$\varphi^{-1}([a]_m, [b]_n) = [bmx + any]_{mn}$$ //

In general we would like to compare rings.

Definition: Given rings R, S we say that a function $\varphi: R \to S$ is a ring homomorphism if

- $\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall\, a, b \in R$
- $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall\, a, b \in R$
- $\varphi(1_R) = \varphi(1_S)$.

Note that $\varphi(a+b) = \varphi(a) + \varphi(b)$ implies that $\varphi(0_R) = 0_S$ because

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$$

Then we can subtract $\varphi(0_R)$ from both sides to get

$$\varphi(0_R) - \varphi(0_R) = \varphi(0_R) + \varphi(0_R) - \varphi(0_R)$$
$$0_S = \varphi(0_R).$$

The same trick does NOT work to prove $\varphi(1_R) = 1_S$ ↓

because $(R, \times, 1)$ is only a semigroup.
So we have to include

$$\varphi(1_R) = 1_S$$

in the definition, because we want it. ///

Properties of homomorphisms:

Given a ring hom $\varphi: R \to S$ we define

$$\operatorname{im}\varphi := \{\varphi(a) : a \in R\} \subseteq S$$
$$\ker\varphi := \{a \in R : \varphi(a) = 0\} \subseteq R$$

Note that the image $\operatorname{im}\varphi$ is a subring of S. Indeed we have $0_S, 1_S \in \operatorname{im}\varphi$ because

$$0_S = \varphi(0_R) \quad \& \quad 1_S = \varphi(1_R).$$

Then for all $\varphi(a), \varphi(b) \in \operatorname{im}\varphi$ we have

$$\varphi(a) + \varphi(a) = \varphi(a+b)$$
$$= \varphi(\text{something})$$

hence $\varphi(a) + \varphi(a) \in \operatorname{im}\varphi$, and

$$\varphi(a)\varphi(b) = \varphi(ab)$$
$$= \varphi(\text{something})$$

hence $\varphi(a)\varphi(b) \in \operatorname{im}\varphi$. ///

Q: Is the kernel $\ker\varphi$ a <u>subring</u> of R?

Let's see. Given $a, b \in \ker\varphi$ we have

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$= 0 + 0 = 0,$$

hence $a+b \in \ker\varphi$, and

$$\varphi(ab) = \varphi(a)\varphi(b)$$
$$= 0 \cdot 0 = 0,$$

hence $ab \in \ker\varphi$. We have seen that

$$\varphi(0_R) = 0_S \implies 0_R \in \ker\varphi.$$

But (WARNING) we probably have

$$1_R \notin \ker \varphi.$$

Indeed, we assumed that $\varphi(1_R) = 1_S$ so we only have $1_R \in \ker \varphi$ when

$$\varphi(1_R) = 1_S = 0_S$$

in which case $S = \{0\}$. Is that even allowed?

So $\ker \varphi$ is not a subring of R. What is it?

Definition: Let R be a ring. A subset $I \subseteq R$ is called an ideal if

- I is a subgroup of $(R, +, 0)$
- $a \in R, x \in I \Rightarrow ax \in I$

"I is closed under multiplication by R, i.e., $RI \subseteq I$"

Theorem: If $\varphi: R \to S$ is a ring hom then $\ker \varphi \leq R$ is an ideal.

Proof: We have seen that $\ker \varphi$ is a subgroup of $(R, +, 0)$. Then for all $a \in R$ and $x \in \ker \varphi$ we have

$$\varphi(ax) = \varphi(a)\varphi(x) = 0 \cdot \varphi(x) = 0$$

hence $ax \in \ker \varphi$. ///

This is analogous to the theory of groups in which kernels of group homs are called normal subgroups.

Analogy:

Group	Ring
Subgroup	Subring
Normal Subgroup	Ideal.

In the case of groups, in fact we have that $H \leq G$ is a normal subgroup if and only if $\exists$ group hom $\varphi: G \to G'$ such that $H = \ker \varphi$.

Why? If $H \leq G$ is normal we construct the quotient group G/H. Then we have a natural group hom

$$\varphi : G \longrightarrow G/H$$
$$g \longmapsto gH$$

with $\ker \varphi = H$

The same thing happens for rings.

Theorem: Let $I \subseteq R$ be a subset of a ring. Then I is an ideal if and only if $\exists$ ring R' and ring hom $\varphi : R \to R'$ such that $I = \ker \varphi$.

Proof: If $\exists\ \varphi : R \to R'$ we have already seen that $\ker \varphi$ is an ideal.

Conversely, suppose that $I \subseteq R$ is an ideal. We want to construct a ring R' and a map $\varphi : R \to R'$ such that $I = \ker \varphi$. HOW?

Since I is a (normal) subgroup of abelian group $(R, +, 0)$ we can form the quotient group

$$R/I := \{ a + I : a \in R \}$$

The elements of R/I are the equivalence classes of the relation

$$a \sim b \iff a - b \in I.$$

This is a group will well-defined operation

$$(a + I) + (b + I) := (a + b) + I$$

and identity $0_{R/I} = 0 + I = I$.

We also have the natural surjective group homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow R/I \\ a &\longmapsto a + I \end{aligned}$$

with $\ker \varphi = I$. Is φ also a ring homomorphism?

Wait a minute! We haven't defined multiplication in R/I. What should it be? We really want

$$\varphi(ab) = (ab) + I = \text{“}\varphi(a)\varphi(b)\text{”} = \text{“}(a+I)(b+I)\text{”}$$

So we just define it that way:

$$(a+I)(b+I) := (ab) + I.$$

This is well-defined because if $a + I = a' + I$ and $b + I = b' + I$ (i.e. $a - a' = x$ and $b - b' = y$ for some $x, y \in I$) then we have

$$\begin{aligned} ab &= (a'+x)(b'+y) \\ &= a'b' + a'y + xb' + xy. \end{aligned}$$

$$ab - a'b' = a'y + xb' + xy \in I.$$

[Here we needed the fact that I is an ideal.]

One can show that

$$(R/I, +, \times, 0+I, 1+I)$$

is a ring, but I won't bother.

In summary, we have constructed a ring R/I (called the quotient ring) and a ring homomorphism

$$\varphi : R \longrightarrow R/I$$
$$a \longmapsto a+I$$

such that $I = \ker \varphi$ 

Thus we have shown that

"ideal" $\equiv$ kernel of ring homomorphism.

Examples:

(1) What are the ideals of $\mathbb{Z}$?

$\downarrow$

We have seen that the only subgroups of $(\mathbb{Z}, +, 0)$ are

$$n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$$

for all $n \in \mathbb{Z}$. Each of these is also an ideal because given $nk \in n\mathbb{Z}$ and $a \in \mathbb{Z}$ we have

$$(nk)a = n(ka) = n(\text{something}) \in n\mathbb{Z}.$$

Thus we can construct the quotient ring

$$\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} : a \in \mathbb{Z}\}$$

as you know....

(2) What are the ideals of the ring of polynomials $\mathbb{R}[x]$?

We'll see later.
For now we'll look at one example.

Consider $x^2+1 \in \mathbb{R}[x]$ and define

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

This is called the principal ideal generated by x^2+1.

Then we can form the quotient ring

$$\mathbb{R}[x]/(x^2+1)$$

Do you recognize this ring?

Claim: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

"Proof": We have declared that

$$x^2+1 = 0$$
$$x^2 = -1.$$

Thus every polynomial can be expressed as $a+bx$, $a, b \in \mathbb{R}$.

Example: $a_0 + a_1 x + a_2 x^2$
$= (a_0 - a_2) + a_1 x$

etc.

Polynomials multiply like this:

$$(a+bx)(c+dx)$$

$$= ac + adx + bcx + bdx^2$$

$$= (ac - bd) + (ad + bc)x$$

Just like complex numbers.

We'll make this formal later.

2/6/14.

HW 2 is due Thurs Feb 20.

Exam 1 will be on Thurs Feb 27.

Last time we defined ideals and constructed the quotient ring.

Def: Let R be a ring. We say that $I \subseteq R$ is an ideal if

- I is a subgroup of $(R, \times, 1)$
- For all $a, b \in R$ we have

$$a \in I \text{ OR } b \in I \implies ab \in I.$$

Theorem: Given $I \subseteq R$ we have

I is an ideal $\iff$ $\exists$ ring R' and hom $\varphi : R \to R'$ with $I = \ker \varphi$.

Proof Idea: $\Leftarrow$ Easy.

$\Rightarrow$ Given ideal $I \subseteq R$ we define the set

$$R/I = \{a + I : a \in R\}.$$

The operations

$$(a+I)+(b+I) := (a+b)+I$$
$$(a+I)(b+I) := (ab)+I$$

are well-defined and make R/I into a ring.
Then we have a natural surjective hom

$$\varphi : R \twoheadrightarrow R/I$$
$$a \longmapsto a+I$$

with $\ker\varphi = I$. //

==

Given a ring R, let

$$\mathcal{L}(R) := \{\text{ideals } I \subseteq R\}$$

be the set of ideals. This set has a nice structure

Given ideals $I, J \in \mathcal{L}(R)$ note that

$I \cap J$ is also an ideal.

Proof: $I \cap J$ is a subgroup of $(R, +, 0)$ because an intersection of subgroups is a subgroup.

Now let $a \in I \cap J$ and $b \in R$. Then we have

$a \in I, b \in R \Rightarrow ab \in I$ and
$a \in J, b \in R \Rightarrow ab \in J$.

Hence $ab \in I \cap J$. //

Q: Is $I \cup J$ an ideal?

NO! $I \cup J$ is not even a subgroup of $(R, +, 0)$.

Example: Consider $2\mathbb{Z}, 3\mathbb{Z} \in \mathcal{L}(\mathbb{Z})$.

Then $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$
and $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$
but $2+3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. //

Definition: Given any subset $S \subseteq R$ we define the ideal generated by S:

$$\langle S \rangle := \bigcap \{ I \in \mathcal{L}(R) : S \subseteq I \}$$

Clearly this is an ideal that contains I. In fact it is the smallest ideal that contains I.

Proof: Suppose $S \subseteq J \in \mathcal{L}(R)$. Then

$$\langle S \rangle = J \cap \{ I \in \mathcal{L}(R) - \{J\} : S \subseteq I \}$$

$$\Rightarrow \langle S \rangle \subseteq J. \quad \blacksquare$$

Given two ideals $I, J \in \mathcal{L}(R)$, the smallest ideal of R containing the union $I \cup J$ is

$$\langle I \cap J \rangle = \{ L \in \mathcal{L}(R) : I \cup J \subseteq L \}.$$

Theorem: For all $I, J \in \mathcal{L}(R)$ we have

$$\langle I \cup J \rangle = I + J$$
$$:= \{ a + b : a \in I, b \in J \}.$$

Proof: Note that $I+J$ is an ideal. It is a subgroup because, given $(a+b), (a'+b') \in I+J$ we have

$$(a+b)-(a'+b') = (a-a')+(b-b') \in I+J$$

because $a-a' \in I$ and $b-b' \in I$. Also, given $a+b \in I+J$ and $c \in R$ we have

$$(a+b)c = ac+bc \in I+J$$

because $ac \in I$ and $bc \in J$.

Now since $I \cup J \subseteq I+J$ we have

$$\langle I \cup J \rangle \subseteq I+J.$$

We want to show $I+J \subseteq \langle I \cup J \rangle$. Indeed, given $a+b \in I+J$ we have $a \in \langle I \cup J \rangle$ and $b \in \langle I \cup J \rangle$. But then

$$a+b \in \langle I \cup J \rangle$$

because $\langle I \cup J \rangle$ is a subgroup. ///

Finally, note that R has a unique maximal ideal

$$(1) = \{1r : r \in R\} = R \quad \text{the "unit ideal"}$$

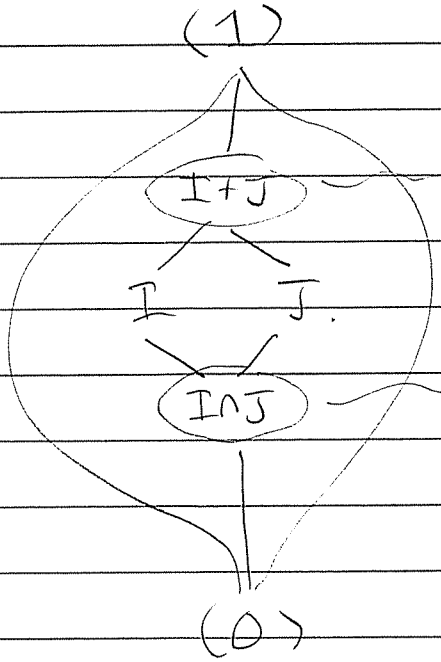
and a unique minimal ideal

$$(0) = \{0r : r \in R\} = \{0\} \quad \text{the "zero ideal"}$$

The structure

$$(\mathcal{L}(R), \cap, +, (0), (1))$$

is called a lattice. Picture:



think $\gcd(I,J)$

think $\text{lcm}(I,J)$.

Example: Recall that the ideals of $\mathbb{Z}$ are just $n\mathbb{Z}$ for all $n \in \mathbb{Z}$. Recall that $\forall\, a, b \in \mathbb{Z}$ we have

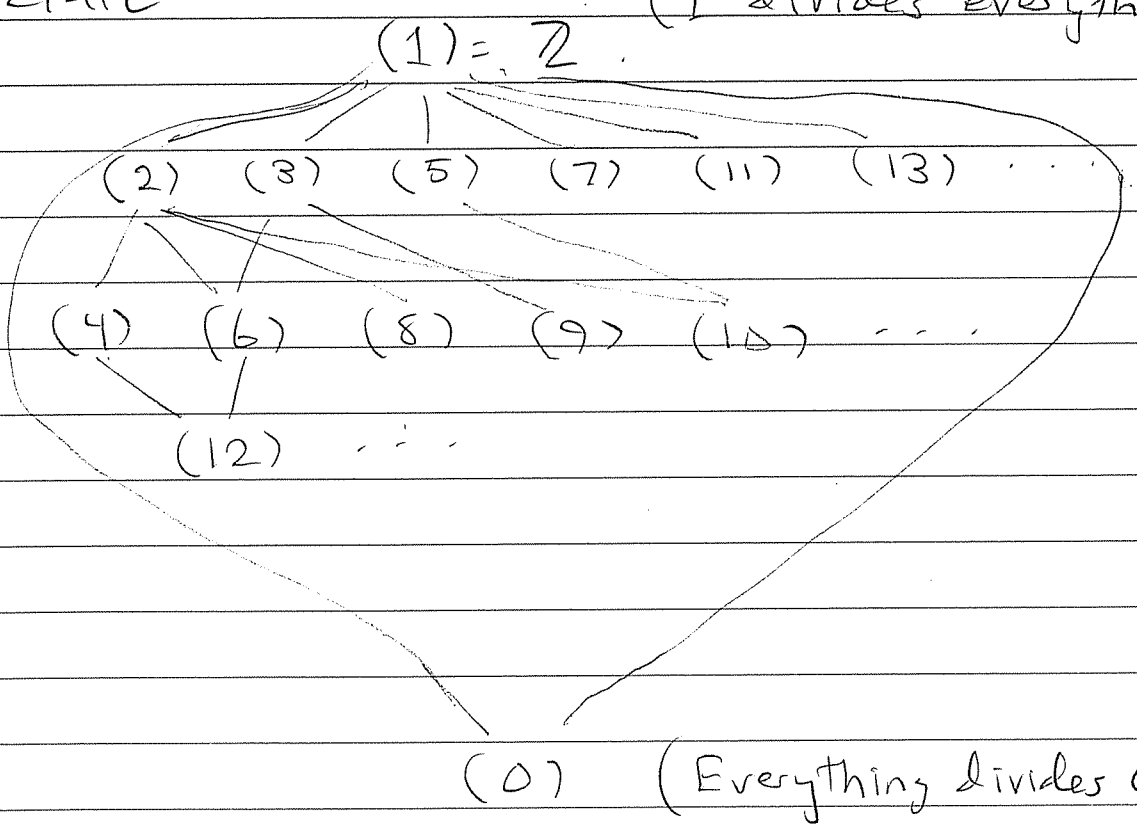
$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$
$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

where $d = \gcd(a,b)$ & $m = \operatorname{lcm}(a,b)$.

Note that we have $a\mathbb{Z} \subseteq b\mathbb{Z} \iff b \mid a$.

[Let's write $(n) := n\mathbb{Z}$ for short.]

Picture:



Q: What is the lattice of ideals of $\mathbb{Z}/n\mathbb{Z}$?

There is a general theorem:

Given ideals $I \subseteq J \subseteq R$ define the set

$$J/I := \{ a + I \; ; \; a \in J \}$$

This is an ideal of R/I because given $a+I, \; b+I \in J/I$ we have

$$(a+I)+(b+I) = (a+b)+I \in J/I$$

because $a+b \in J$ and given $(a+I) \in J/I$ and $(b+I) \in R/I$ we have

$$(a+I)(b+I) = (ab)+I \in J/I$$

because $ab \in J$. Define

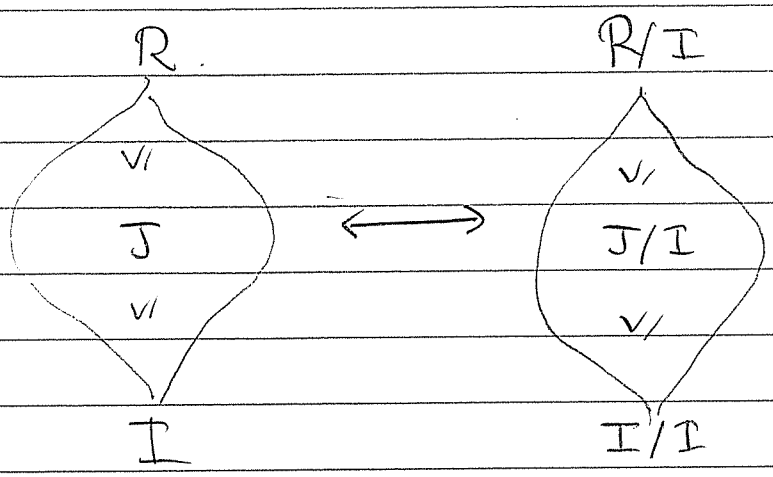
$$\mathcal{L}(R, I) := \{ \text{ideals } I \subseteq J \subseteq R \}$$

Then we have a map

$$\mathcal{L}(R, I) \longrightarrow \mathcal{L}(R/I).$$

defined by $J \longmapsto J/I$.

✡ Correspondence Theorem: This map is an isomorphism of lattices



$\mathcal{L}(R, I) \longleftrightarrow \mathcal{L}(R/I)$.

Proof omitted ☹ //

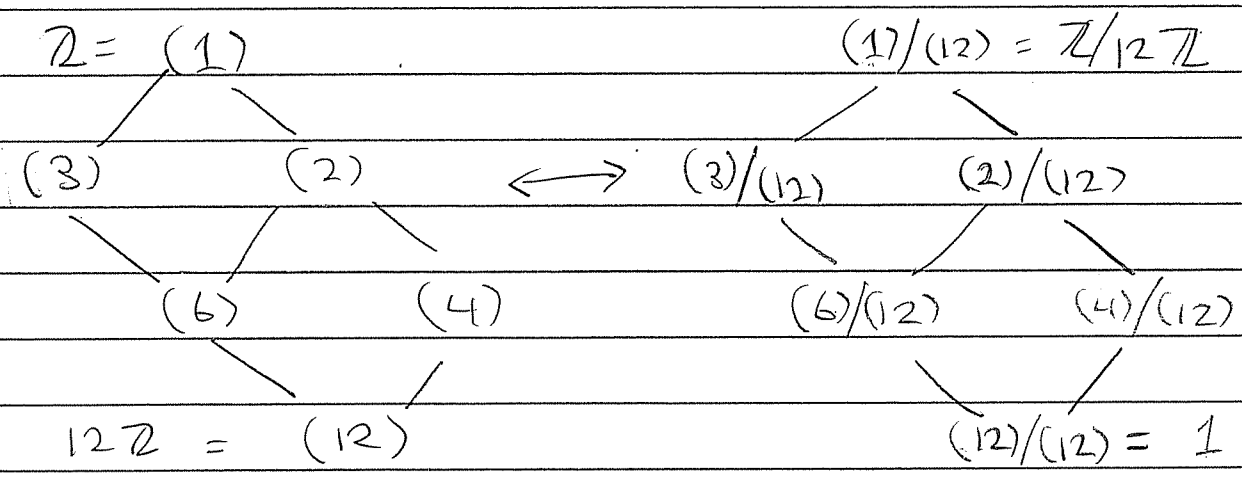
There is a fun corollary of this.

✡ Fundamental Theorem of cyclic groups:

$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \cong$ lattice of divisors of the integer n.

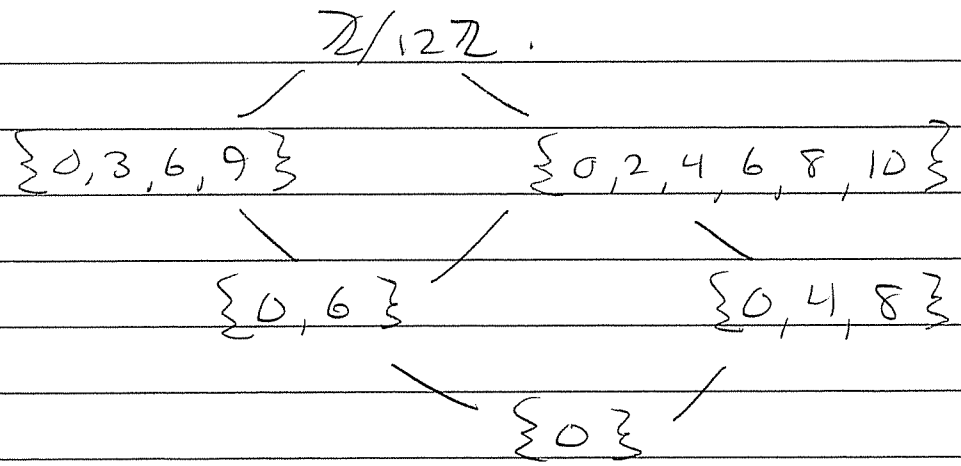
Proof: $\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \approx \mathcal{L}(\mathbb{Z}, n\mathbb{Z})$ ///

Example: $\mathbb{Z}/12\mathbb{Z}$.



You may have heard it like this:

For every $d|n$ there is a unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d.



We end with the important

★ "First Isomorphism Theorem":

Given any ring homomorphism

$$\varphi : R \longrightarrow R'$$

we can turn it into a ring isomorphism in a natural way.

We make it surjective by restricting to the image

$$\varphi : R \longrightarrow \operatorname{im}\varphi.$$

Then we make it injective by killing the kernel

$$\overline{\varphi} : R/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi.$$
$$a + \ker\varphi \longmapsto \varphi(a).$$

Proof: Clearly $\overline{\varphi}$ is a surjective ring homomorphism.

↳

We need to check that $\overline{\varphi}$ is injective and well-defined. Note that

$$a + \ker\varphi = b + \ker\varphi \iff a - b \in \ker\varphi$$
$$\iff \varphi(a-b) = 0$$
$$\iff \varphi(a) - \varphi(b) = 0$$
$$\iff \varphi(a) = \varphi(b).$$

$\Longrightarrow$ proves well-defined

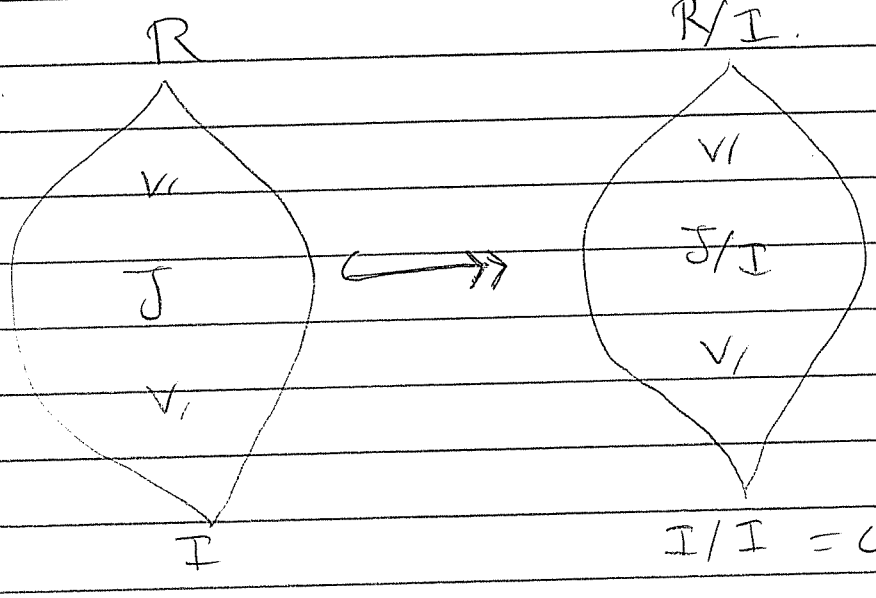
$\Longleftarrow$ proves injective.

2/11/14

HW 2 due Thurs Feb 20
McKnight - Zome Lecture Wed 5:30

Last time we discussed the

✡ Correspondence Theorem for Rings:
Given an ideal $I \leq R$, the map $J \mapsto J/I$ defines a lattice isomorphism from ideals $I \leq J \leq R$ to ideals $J/I \leq R/I$:



$$\mathcal{L}(R, I) \cong \mathcal{L}(R/I)$$

Application:
Fundamental Theorem of Cyclic Groups

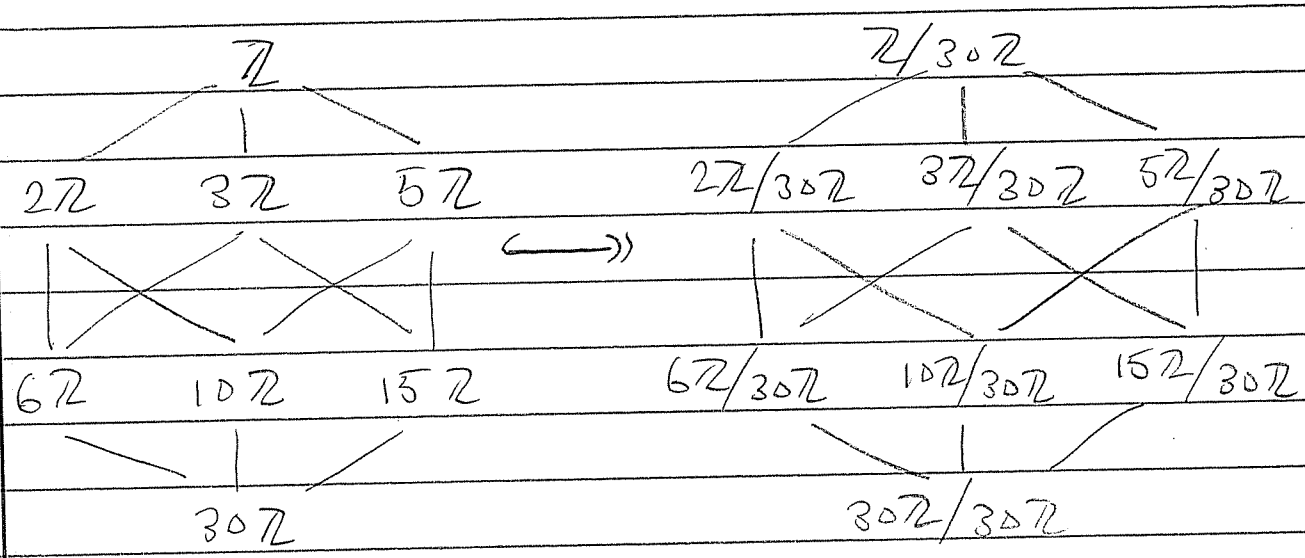
For all $n \in \mathbb{Z}$ we have

$$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \approx \text{lattice of divisors } d \mid n$$

Proof: we have

$$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \approx \mathcal{L}(\mathbb{Z}, n\mathbb{Z}) \approx \text{what we want}$$ ///

Example: $\mathbb{Z}/30\mathbb{Z}$



where, for example,

$$5\mathbb{Z}/30\mathbb{Z} = \{0, 5, 10, 15, 20, 25\} \leq \mathbb{Z}/30\mathbb{Z}.$$

//

Recall that a ring homomorphism $\varphi: R \to R'$ satisfies

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_{R'}$

We say that φ is a ring isomorphism if it is surjective (i.e. $\operatorname{im}\varphi = R'$) and injective (i.e. $\varphi(a) = \varphi(b) \Rightarrow a = b$).

Lemma: we have

φ is injective $\iff \ker\varphi = 0$.

Proof: Suppose φ is injective. Then for all $a \in \ker\varphi$ we have

$$\varphi(a) = 0 = \varphi(0) \implies a = 0.$$

Hence $\ker\varphi = 0$. Conversely, suppose that $\ker\varphi = 0$. If $a, b \in R$ satisfy

$$\varphi(a) = \varphi(b)$$

then we have

$$\varphi(a-b) = \varphi(a) - \varphi(b) = 0$$

$\Rightarrow a-b \in \ker\varphi \Rightarrow a-b = 0 \Rightarrow a = b.$

Hence φ is injective ///

This leads to the important

★ First Isomorphism Theorem
(Emmy Noether, 1927) :

Given any ring homomorphism $\varphi: R \to R'$
we can turn it into a ring isomorphism
in a natural way.

We make it surjective by restricting
to the image

$$\varphi : R \twoheadrightarrow \operatorname{im}\varphi.$$

Then we make it injective by killing
the kernel

↓

$\bar{\varphi} : R/\ker\varphi \hookrightarrow \text{im}\,\varphi$

$a + \ker\varphi \longmapsto \varphi(a)$

Proof: Clearly $\bar{\varphi}$ is a surjective ring homomorphism. We need to check that $\bar{\varphi}$ is well-defined and injective.

Note that

$$\begin{aligned} a+\ker\varphi = b+\ker\varphi &\iff a-b \in \ker\varphi \\ &\iff \varphi(a-b) = 0 \\ &\iff \varphi(a) - \varphi(b) = 0 \\ &\iff \varphi(a) = \varphi(b) \end{aligned}$$

$\Rightarrow$ proves well-defined

$\Leftarrow$ proves injective. 

Application: Evaluation of polynomials.

Recall: Given any ring R we define the ring of polynomials

$$R[x] := \{ a_0 + a_1 x + a_2 x^2 + \cdots : a_i \in R \text{ and } a_i = 0 \text{ for all but finitely many } i \}$$

At first a polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is just an abstract expression, but we can turn it into a function as follows.

Consider any ring $S \supseteq R$ (called an extension ring of R) and any element $\alpha \in S$. Then we have

★ **Evaluation Theorem:** There exists a unique ring homomorphism $R[x] \to S$ sending $a \mapsto a$ for all $a \in R$ and sending $x \mapsto \alpha$.

Proof: Define the map

$$ev_\alpha\left(\sum_k a_k x^k\right) := \sum_k a_k \alpha^k \in S$$

It is easy to check (HW 2) that $ev_\alpha : R[x] \to S$ is a ring homomorphism with $ev_\alpha(x) = \alpha$ and $ev_\alpha(a) = a \ \forall a \in R$.

Now let $\varphi : R[x] \to S$ be any ring hom with $\varphi(x) = \alpha$ and $\varphi(a) = a \quad \forall a \in R$.
Then we have

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

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

Hence $\varphi = ev_\alpha$. //

We call this map "evaluation at α" and we write

$$ev_\alpha(f(x)) = \text{“}f(\alpha)\text{”}$$

even though it may cause confusion for beginners.

Definition: Let $R \subseteq S$ be a ring extension with $\alpha \in S$, and consider the evaluation map

$$ev_\alpha : R[x] \to S.$$

Then we define

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

Note that $R[\alpha]$ is a subring of S containing R:

$$R \subseteq R[\alpha] \subseteq S.$$

In fact, $R[\alpha]$ is the smallest subring of S containing $R \cup \{\alpha\}$.

Theorem: Given $R \subseteq S$ and $\alpha \in S$ we define

$$\langle R \cup \{\alpha\} \rangle := \bigcap \{\text{subrings } T \subseteq S : R \cup \{\alpha\} \subseteq T\}$$

Then we have $R[\alpha] = \langle R \cup \{\alpha\} \rangle$.

Proof: Since $R[\alpha]$ is a subring of S containing $R \cup \{\alpha\}$ we have

$$\langle R \cup \{\alpha\} \rangle = R[\alpha] \cap \{\text{others}\}$$

$$\langle R \cup \{\alpha\} \rangle \subseteq R[\alpha]$$

Conversely, since $\langle R \cup \{\alpha\} \rangle$ is a ring containing $R \cup \{\alpha\}$ it also contains

$$\sum_k a_k \alpha^k \quad \text{for all } a_k \in R.$$

Hence $R[\alpha] \subseteq \langle R \cup \{\alpha\} \rangle$ ///

Definition: The ring $R[\alpha]$ is called

"R adjoin α"

The First Isomorphism Theorem tells us that given

$$ev_\alpha : R[x] \longrightarrow R[\alpha] \subseteq S$$

we have

$$\frac{R[x]}{\ker(ev_\alpha)} \cong im(ev_\alpha) = R[\alpha].$$

Thus $R[\alpha]$ is a quotient of $R[x]$

What is the kernel?

Example: Consider $\mathbb{R} \subseteq \mathbb{C}$ and $i \in \mathbb{C}$. Then

$$ev_i : \mathbb{R}[x] \longrightarrow \mathbb{C}$$

is surjective hence $\mathbb{R}[i] = \mathbb{C}$.
The kernel is

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

You will prove on HW 2 that

$$f(i) = 0 \implies f(x) = (x - i)\, g(x)$$

where $\deg(g) = \deg(f) - 1$.

But note that complex conjugation is a ring isomorphism $\mathbb{C} \to \mathbb{C}$. hence for all $f(x) \in \mathbb{R}[x]$ and $z \in \mathbb{C}$ we have

$$\overline{f(z)} = f(\overline{z}).$$

In particular we have

$$f(-i) = \overline{f(i)} = \overline{0} = 0.$$

hence $-i$ is also a root of $f(x)$

$$f(x) = (x-i)\,g(x)$$
$$f(-i) = (-i-i)\,g(-i) = 0$$
$$-2i\,g(-i) = 0$$

$$\Rightarrow \quad g(-i) = 0.$$

$$\Rightarrow \quad g(x) = (x+i)\,h(x)$$

where $\deg(h) = \deg(g) - 1$

Hence

$$f(x) = (x-i)(x+i)\,h(x)$$
$$f(x) = (x^2+1)\,h(x)$$

Note that $h(x)$ has <u>real</u> coefficients (Why?) so we conclude that

$(x^2+1) \mid f(x)$ in the ring $\mathbb{R}[x]$.

Conversely, any $f(x)$ divisible by x^2+1 is in the kernel of ev$_i$.

We conclude that

$$\ker(ev_i) = (x^2+1)$$
$$= \{(x^2+1)h(x) : h(x) \in \mathbb{R}[x]\},$$

the principal ideal generated by x^2+1.
And hence

$$\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{C}.$$

This is the "grown-up" definition of $\mathbb{C}$.

2/12/14

HW 2 due Thurs Feb 20

Last time we proved Emmy Noether's

★ First Isomorphism Theorem:
Given any ring homomorphism

$$\varphi : R \longrightarrow R'$$

we obtain a ring isomorphism

$$\bar{\varphi} : R/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$$
$$a + \ker\varphi \longmapsto \varphi(a).$$

Proof:

$$a + \ker\varphi = b + \ker\varphi \iff a - b \in \ker\varphi$$
$$\iff \varphi(a-b) = 0$$
$$\iff \varphi(a) - \varphi(b) = 0$$
$$\iff \varphi(a) = \varphi(b)$$

//

We applied this to the evaluation of polynomials:

Given rings $R \subseteq S$ and element $\alpha \in S$ we have a unique evaluation map

$$ev_\alpha : R[x] \longrightarrow S$$
$$f(x) \longmapsto f(\alpha).$$

The image is the smallest subring of S containing R and α. Notation:

$$R[\alpha] := im(ev_\alpha) \quad \text{"}R \text{ adjoin } \alpha\text{"}.$$

Using the First Isomorphism Theorem we have

$$R[\alpha] \approx R[x] / \ker(ev_\alpha).$$

This is an interesting idea because it allows us to create ring extensions out of thin air:

Recall that $2x - 1 \in \mathbb{Z}[x]$ has no root in $\mathbb{Z}$, i.e., "$1/2$" $\notin \mathbb{Z}$.

We're not satisfied with that,

so we define the principal ideal.

$$(2x-1) := \{(2x-1)f(x) : f(x) \in \mathbb{Z}[x]\}$$

and consider the quotient ring

$$R := \mathbb{Z}[x]/(2x-1)$$

Note that the map $\mathbb{Z} \xrightarrow{\iota} R$ defined by $a \longmapsto a + (2x-1)$ is an injective ring homomorphism. Indeed, given $a, b \in \mathbb{Z}$ we have

$$a + (2x-1) = b + (2x-1)$$
$$\Rightarrow a - b \in (2x-1)$$
$$\Rightarrow a - b = (2x-1)(a_0 + a_1 x + \cdots + a_n x^n)$$

$$\Rightarrow a - b = -a_0 + (2a_0 - a_1)x + \cdots + (2a_{n-1} - a_n)x^n + 2a_n x^{n+1}$$

Since these polynomials are equal, by definition the coefficients must be equal. Hence

$$2a_n = 0 \implies a_n = 0$$
$$2a_{n-1} - a_n = 0 \implies a_{n-1} = 0$$
$$2a_{n-2} - a_{n-1} = 0 \implies a_{n-2} = 0$$
$$\vdots$$
$$2a_0 - a_1 = 0 \implies a_0 = 0$$
$$-a_0 = a - b \implies a - b = 0$$
$$\implies a = b.$$

Thus $\iota : \mathbb{Z} \to R$ is an injection (i.e. $\ker(\iota) = (0)$) and by FII we have

$$\mathbb{Z}/(0) = \mathbb{Z} \approx \operatorname{im}(\iota) \subseteq R$$

By abuse of notation we will often just write

$$\mathbb{Z} = \operatorname{im}(\iota) \subseteq R$$

and say $\mathbb{Z}$ is a subring of R, even though this is confusing for beginners ^^

Thus we have defined a ring extension $\mathbb{Z}$ with a special property:

The polynomial $2x - 1 \in \mathbb{Z}[x]$ has a solution in R.

Proof: Let $f(x) = 2x - 1 \in \mathbb{Z}[x]$ and consider the element $\alpha = x + (2x - 1) \in R$. I claim that $f(\alpha) = 0$ (i.e., we might say that "$\alpha = 1/2$"). Indeed, by definition of the evaluation morphism we have

$$\begin{aligned} f(\alpha) &= (2 + (2x-1))(x + (2x-1)) - (1 + (2x-1)) \\ &= 2x - 1 + (2x - 1) \\ &= 0 + (2x - 1) \\ &= 0_R \end{aligned}$$

That was a lot of nonsense, so let me say why we might care.

Prior to 1830,

"Algebra" $\equiv$ "Trying to solve polynomial equations"

Example: The equation

$$ax^2 + bx + c = 0$$

has solutions $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$,

but now we have to grapple with square roots.

Example: The equation

$$x^3 + px + q = 0$$

has at least one solution given by.

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

"Cardano's Formula" (1545).

But now we have to grapple with cube roots.

Cardano's student Ferrari gave a formula for roots of quartic equations. But then people got stuck.

★ Theorem (Abel, 1824):
There is no nice formula for the roots of a quintic equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

Great, but what does "nice formula" mean?

Then there was an earthquake named Galois (~1830).

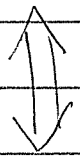
Let R be a ring and consider a polynomial $f(x) \in R[x]$. We can artificially construct a ring extension $R \subseteq S$ in which $f(x) = 0$ is completely solvable. The abstract-algebraic properties of $R \subseteq S$ tell us what kind of "formulas" to expect for the roots.

The punchline: Let K be a field and consider a polynomial $f(x) \in K[x]$. Then we can construct a field $K \subseteq L$ in which $f(x)$ has all its roots.

Define the Galois group of the extension

$$\mathrm{Gal}(K \subseteq L) := \{ \text{ring isomorphisms } \sigma : L \to L \text{ such that } \sigma(k) = k \ \forall k \in K \}.$$

Then the equation $f(x) = 0$ is solvable "by radicals", i.e. only using $+, \times, -, \div, \sqrt{}, \sqrt[3]{}, \sqrt[4]{}, \ldots$



The group $\mathrm{Gal}(K \subseteq L)$ has a chain of normal subgroups

$$\mathrm{Gal}(K \subseteq L) \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\}$$

with the property that G_i / G_{i+1} is abelian for all i.

In the process, Galois invented "groups", "normal subgroups" and "quotient groups".

The fact that the general quintic is not solvable "by radicals" is then proved as follows:

The typical quintic has Galois group $\approx S_5$ (permutations of 5 things).

But S_5 contains a big simple nonabelian subgroup (the icosahedral group):

$$S_5 \rhd \text{icosahedron} \rhd \{1\}$$

↑

This icosahedron is in the way!

Of course the general quintic is solvable, just not "by radicals".

It can be solved with "elliptic functions" (Felix Klein, "Lectures on the icosahedron", 1884)

2/18/14

HW 2 due this Thurs Feb 20
Exam 1 next Thurs Feb 27

Recall from last time:

Let $f(x) \in K[x]$ be a polynomial of degree n over a field K. If $f(x) = 0$ has no solution we can abstractly create a solution by defining

$$K' := K[x]/(f(x))$$

By abuse of notation we can say $K \subseteq K'$ by identifying $a \in K$ with $a + (f(x)) \in K'$. Note that $\alpha := x + (f(x))$ is a root of f because

$$\begin{aligned} ev_\alpha(f(x)) &= f(x + (f(x))) \\ &= f(x) + (f(x)) \\ &= 0 + (f(x)) \\ &= 0_{K'}. \end{aligned}$$

Then we can use Descartes' Factor Theorem to write

$$f(x) = (x-\alpha)\, g(x) \in K'[x]$$

with $\deg(g) = n-1$. If $g(x) = 0$ has no solution we repeat the construction

$$K'' := K'[x]/(g(x)).$$

to obtain a chain of fields

$$K \subseteq K' \subseteq K'' \subseteq \cdots.$$

The process must stop since the degree of the polynomial is going down, so we obtain a field $K \subseteq L$ in which

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n) \in L[x].$$

called the splitting field of $f(x)$.

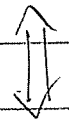
Define the Galois group of $K \subseteq L$

$$\mathrm{Gal}(K \subseteq L) := \{ \text{ring isomorphisms } \sigma : L \to L \text{ such that } \sigma(k) = k \ \forall k \in K \}$$

Then we have

Theorem (Galois, ~1830):

The equation $f(x) = 0$ is solvable "by radicals", i.e., using only $+, -, \times, \div$, $\sqrt{}, \sqrt[3]{}, \sqrt[4]{}, \ldots$



The group $\mathrm{Gal}(K \subseteq L)$ has a chain of normal subgroups

$$\mathrm{Gal}(K \subseteq L) \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{1\}$$

such that G_i / G_{i+1} is abelian for all i.
In this case we say the group $\mathrm{Gal}(K \subseteq L)$ is "solvable".

In this course I hope to appreciate what Galois did.

End of Culture. Back to details.

Let R be a ring. To study quotients $R[x]/I$ we must first study ideals $I \subseteq R[x]$. What are they?

Note: If $I \subseteq R$ is an ideal then the set $I[x] \subseteq R[x]$ is an ideal, so we should choose R with very few ideals. Every ring R has at least two ideals

$(0) \subseteq R$ the zero ideal
$(1) = R$ the unit ideal

Theorem: Let R be a ring. Then

R is a field $\iff$ R has exactly two ideals $(0), (1) \subseteq R$.

Proof: Suppose R is a field and let $I \subseteq R$ be an ideal. If $I \neq (0)$ then there exists $0 \neq a \in I$. Since R is a field we have $a^{-1} \in R$ and then since I is an ideal we have

$$1 = a a^{-1} \in I$$
$$\uparrow \quad \uparrow$$
$$\in I \quad \in R$$

Finally since $1 \in I$ we have $I = (1)$ [Why?]

Conversely, suppose that R has exactly two ideals (0) & (1), and consider any $0 \neq a \in R$. Since $(a) \neq (0)$ we must have $(a) = (1)$. Then since $1 \in (a)$, there exists $b \in R$ such that $1 = ab$. We conclude that R is a field. ///

This suggests we should first look at ideals of $K[x]$ where K is a field.

✡ **Theorem**: Every ideal of $K[x]$ has the form

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

for some polynomial $f(x) \in K[x]$.

[Jargon: We say that $K[x]$ is a principal ideal domain (PID)]

Q: How can we prove this?

A: How did we prove that $\mathbb{Z}$ is a PID? (i.e. every ideal is (n) for some $n \in \mathbb{Z}$)

Recall the Proof:

Let $I \subseteq \mathbb{Z}$ be any ideal. If $I = (0)$ we're done so suppose that $I \neq (0)$. Then by well-ordering $\exists\ 0 \neq n \in I$ with $|n|$ minimum.

Claim: $I = (n)$. Indeed, since $n \in I$ we have $(n) \subseteq I$. Then given any $m \in I$ we can divide by n to obtain

- $m = qn + r$
- $r = 0$ or $0 < |r| < |n|$

If $0 < |r| < |n|$ then since $r = m - qn$ is in I, we obtain a contradiction to the minimality of n. We conclude that $r = 0$, hence $m \in (n)$, hence $I \subseteq (n)$.

The "same" proof will work for $K[x]$ if we can do division with remainder.

Can we?

Definition: Given a ring R and a polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in R[x],$$

let $\deg(f)$ be the maximum n such that $a_n \neq 0$. We will say that $f(x)$ is a monic polynomial if its leading coefficient is a unit (i.e. if a_n^{-1} exists).

☆ **Theorem:** Let R be a ring. Given $f, g \in R[x]$ with $g(x)$ monic, there exist $q, r \in R[x]$ such that

- $f(x) = q(x)g(x) + r(x)$
- $r(x) = 0$ OR $\deg(r) < \deg(g)$.

[Q: What is the degree of the zero polynomial? Why?]

Proof by Example:

Consider $f(x) = 2x^3 + 3x + 1$ } in $\mathbb{Z}[x]$
$g(x) = x + 1$
↑ monic. ✓

Then we have

$$\begin{array}{r|l} & 2x^2 - 2x + 5 \\ \hline x+1 & 2x^3 + 0x^2 + 3x + 1 \\ & 2x^3 + 2x^2 \quad\quad \\ \hline & -2x^2 + 3x + 1 \\ & -2x^2 - 2x \quad\quad \\ \hline & 5x + 1 \\ & 5x + 5 \\ \hline & -4. \end{array}$$

$\Rightarrow$ $(2x^3 + 3x + 1) = \underbrace{(2x^2 - 2x + 5)}_{q(x)}(x+1) + \underbrace{(-4)}_{r(x)}$

Note that $\deg(-4) < \deg(x+1)$
$0 \qquad\qquad 1$

What happens if $g(x)$ is not monic?

Let $g(x) = 2x + 1 \in \mathbb{Z}[x]$. Then

$$
\begin{array}{r|l}
 & x^2 - \frac{1}{2}x + \frac{7}{4} \\
\hline
2x+1 & 2x^3 + 0x^2 + 3x + 1 \\
 & 2x^3 + x^2 + 0 + 0 \\
\hline
 & -x^2 + 3x + 1 \\
 & -x^2 - \frac{1}{2}x + 0 \\
\hline
 & \frac{7}{2}x + 1 \\
 & \frac{7}{2}x + \frac{7}{4} \\
\hline
 & -\frac{3}{4}
\end{array}
$$

The quotient and remainder are in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$ ☹ ///

Remark: If K is a field then

$f(x) \in K[x]$ is monic $\iff$ $f(x) \neq 0$.

So we can divide by any nonzero polynomial.

It follows that $K[x]$ is a PID.

[Exercise: Write out the proof of this.]

Recall: I said that there is a deep analogy between

$$\mathbb{Z} \quad \& \quad K[x].$$

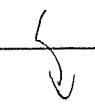
This is expressed by the concept of a PID. But $\mathbb{Z}$ also has unique factorization.

Definition: Let R be a domain, i.e., suppose that $\forall\, a, b \in R$ we have

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

We say that $a \in R$ is irreducible if $\forall\, b, c \in R$ we have

$$a = bc \implies b \text{ or } c \text{ is a unit.}$$



We say that R is a unique factorization domain (UFD) if

- every element is a product of irreducibles, times a unit.
- this expression is unique up to reordering irreducibles and multiplying by units.

Q: Since $\mathbb{Z}$ is a UFD, maybe $K[x]$ is also a UFD?

How can we prove it?

A: We will show more generally that any PID is a UFD.

That will give us a better understanding of why it's true.

2/20/14

HW 2 due NOW
Exam 1 next Thurs Feb 27
I am out of town March 4 & 6 ☹

Let R be a ring. We say R is a domain (sometimes called an "integral domain") if it has no zero divisors, i.e., if for all $a, b \in R$ we have

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

You will show on HW3 that

domain $\equiv$ subring of a field

The main example of a non-domain is a direct product of rings

$$R \times S := \{(r, s) : r \in R, s \in S\}.$$

It is not a domain because

$$(1_R, 0_S) \cdot (0_R, 1_S) = (0_R, 0_S)$$

But $(1_R, 0_S), (0_R, 1_S) \neq 0_{R \times S}$

Example: $\mathbb{Z}/6\mathbb{Z}$ is not a domain because

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

The main example of a domain is $\mathbb{Z}$.

Now here is a silly definition:

Let R be a domain. We say that R is a Euclidean Domain if $\exists$ "size" function $\delta : R-0 \to \mathbb{N}$ such that $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ such that

- $a = qb + r$
- $r = 0$ OR $\delta(r) < \delta(b)$.

There are really just two Examples

(1) $R = \mathbb{Z}$ with size function $\delta(n) = |n|$.

(2) $R = K[x]$ with K a field and size function $\delta(f) = \text{degree}(f)$.

The proofs that $\mathbb{Z}$ and $K[x]$ are Euclidean are similar but not the same. Both are described by an ALGORITHM (called a "Euclidean Algorithm").

Definition: A domain R is called a PID (principal ideal domain) if every ideal $I \leq R$ is generated by a single element $a \in R$:

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

Theorem: Euclidean $\Rightarrow$ PID

Proof: Let R be Euclidean and consider any ideal $I \leq R$. If $I = (0)$ we're done. If not, there exists nonzero $a \in I$ with minimum size $\delta(a)$.
Claim: $I = (a)$. Indeed since $a \in I$ we have $(a) \leq I$. Conversely, consider any $b \in I$. Since $a \neq 0$ we can divide to get

- $b = qa + r$
- $r = 0$ or $\delta(r) < \delta(a)$.

Since $a, b \in I$ and $q \in R$ we have

$$r = b - qa \in I$$

If $r \neq 0$ this contradicts the minimality of $a \in I$. Hence $r = 0$ and we conclude that $b = qa \in (a)$; i.e., $I \subseteq (a)$.

Hence $I = (a)$. ▨

Corollary: $\mathbb{Z}$ and $K[x]$ are PIDs.

The language of PIDs is elegant:

Let R be a PID. Then

$(a) = (1) \iff a$ is a unit.

Proof: If $(a) = (1)$ then $1 \in (a) \Rightarrow$
$1 = ab \Rightarrow a$ is a unit.
Conversely if a is a unit then

$$1 = a a^{-1} \in (a).$$

Hence $(1) \subseteq (a)$. But clearly

$(a) \leq (1)$ so we have $(a) = (1)$ ///

More generally we have

$(a) \leq (b) \iff b$ divides a

Proof: Suppose that $(a) \leq (b)$. Then

$a \in (b) \Rightarrow a = bc$ for some $c \in R$

$\Rightarrow b$ divides a.

Conversely, if $a = bc$ for some c

then $a \in (b) \Rightarrow (a) \leq (b)$ ///

Q: What does $(a) = (b)$ mean?

Suppose $(a) = (b)$. Then

$a \in (b) \Rightarrow a = bc$ for some $c \in R$

$b \in (a) \Rightarrow b = ad$ for some $d \in R$.

This implies that

$$a = bc$$
$$a = (ad)c$$
$$a = a(dc)$$
$$a(1 - dc) = 0.$$

If $a \neq 0$ then since R is a domain this implies

$$1 - dc = 0$$
$$1 = dc.$$

i.e. d and c are units.

Definition: We say $a, b \in R$ are associates if they differ by a unit, i.e, if $a = bu$ for some unit $u \in R^\times$

[Recall: $(R^\times, 1, \times)$ is the group of units.]

Then we have

$(a) = (b) \iff a, b$ are associates.

Proof: Let $(a) = (b)$. We saw that this implies $a = bc$ where $c \in R^\times$.

Conversely, suppose $a = bu$ with $u \in R^\times$. Then

$a = bu \implies a \in (b) \implies (a) \leq (b)$

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

//

Examples:

- Recall that $\mathbb{Z}^\times = \{\pm 1\}$ so we have

$$(n) = (-n) \quad \forall\, n \in \mathbb{Z}.$$

- Let K be a field. What are the units of $K[x]$?

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

$$\deg(fg) = \deg(f) + \deg(g).$$

Thus if $f(x)g(x) = 1$ we have

$$\deg(f) + \deg(g) = \deg(1) = 0.$$

Since $\deg(f), \deg(g) \geq 0$ this implies that

$$\deg(f) = \deg(g) = 1.$$

We conclude that

$$(K[x])^\times = K^\times$$

(nonzero constants)

Thus given $f(x), g(x) \in K[x]$ we have

$$(f(x)) = (g(x)) \iff f(x) = kg(x) \text{ for some } k \in K^{\times}.$$

In particular, every ideal $I \leq K[x]$ can be written uniquely as

$$I = (f(x))$$

where $f(x) = 1x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

Q: What does it mean to say that $f(x) \in K[x]$ is irreducible?

A: We say $f(x)$ is irreducible if

$f(x) = g(x)h(x) \implies g(x)$ or $h(x)$ is a nonzero constant.

"It cannot be factored"

Example: $x^2 + 1 \in \mathbb{R}[x]$ is irreducible.

$x^2 + 1 \in \mathbb{C}[x]$ is reducible,

$$x^2 + 1 = (x - i)(x + i)$$

///

Definition: In a ring R we say that element $a \in R$ is irreducible if

$$a = bc \implies b \text{ or } c \text{ is a unit}$$

We say $a \in R$ is reducible if

$$a = bc$$

where b, c are not units and not associate to a. In this case we say b, c are proper divisors of a.

In the language of ideals:

$(a) < (b) < (1)$ $\iff$ • b divides a
• b not a unit
• b not associate to a

☆ **Theorem**: In a PID we have

$a \in R$ is irreducible

$\iff$ (a) is a maximal ideal.

Proof: Suppose $a \in R$ is irreducible and consider the ideal (a). Suppose for contradiction there exists an ideal

$$(a) < I < (1).$$

Since R is PID we have $I = (b)$ and then b is a proper divisor of a, contradicting the fact that a is irreducible. Hence (a) is maximal.

Conversely, suppose that (a) is a maximal ideal and suppose that

$$a = bc.$$

Then $a \in (b) \Rightarrow (a) \leq (b)$. If $(a) = (b)$ then we're done, so suppose that $(a) < (b)$. Since (a) is maximal this implies $(b) = (1)$. Hence b is a unit. We conclude that a is irreducible.

There is another nice way to say this.

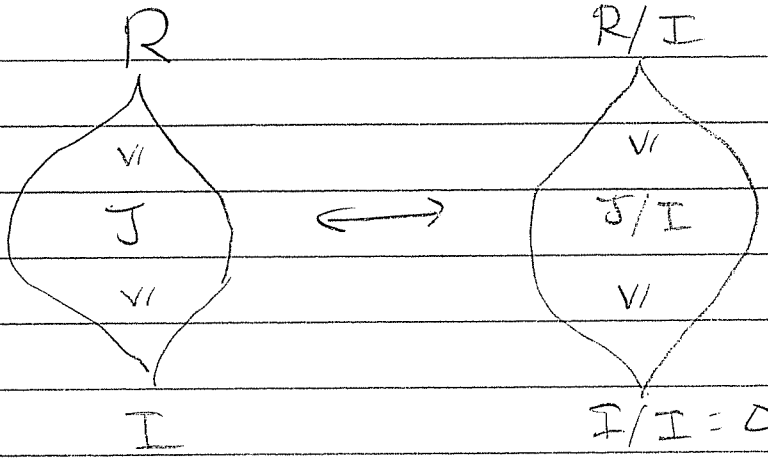
Let R be any ring (maybe not PID).
we say an ideal $I \subseteq R$ is maximal if.

- $I \neq R$.
- $I \subseteq J \subseteq R \implies J = I$ or $J = R$.

☆ Theorem: Let $I \subseteq R$ be an ideal. Then

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

Proof: Recall the Correspondence Thm.



I is maximal $\iff \mathcal{L}(R, I) = \{R, I\}$
$\iff \mathcal{L}(R/I) = \{R/I, 0\}$
$\iff R/I$ is a field

Here's a fun application:

The polynomial $x^2+1 \in \mathbb{R}[x]$ is irreducible.

Proof: From HW 2 you know that

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

Since $\mathbb{C}$ is a field, the ideal (x^2+1) is maximal. Since $\mathbb{R}[x]$ is a PID this implies that the polynomial $x^2+1 \in \mathbb{R}[x]$ is irreducible. //

On the other hand: If you somehow know that $f(x) \in K[x]$ is irreducible, you will automatically know that

$K[x]/(f(x))$ is a field

Example: $x^2+x+1 \in \mathbb{Z}/(2)[x]$ ...