Welcome back

We are all in this together and we will get through this together.

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 7.6–7.7; for Mon: 8.1.
- PS08: Due Mon. (But deadlines are elastic.)
- Exam 2 (tentatively) on Wed Apr 22; done on paper, submitted by Canvas, proctored by Zoom. (First rehearsal: Last 5 min of class today.)
- Monday's DJ: Xiyuan; Today's DJ: Rudra.

Outline for PS08 due tomorrow.

Problem session on Fri on PS08 (or whatever)

Last: Homomorphisms and isomorphisms

Definition

Let R and R' be rings. To say that a function $\varphi : R \to R'$ is a **homomorphism** means that for all $r, s \in R$,

$$\varphi(r+s) = \varphi(r) + \varphi(s), \qquad \varphi(rs) = \varphi(r)\varphi(s).$$

ie, phi preserves addition and multiplication.

Definition

An **isomorphism** is a bijective (one-to-one and onto) homomorphism. To say that rings R and R' are **isomorphic** means that there exists some isomorphism $\varphi : R \to R'$. think: renaming

Think: Isomorphic functions are, abstractly, the same ring with different names. (of elements).

End of last time: Examples of how to show rings are *not* isomorphic.

Automorphisms

homo: similar, alike
iso: same
auto: self

Definition

An **automorphism** is an isomorphism $\varphi : R \to R$ from a ring to itself.

(complex conjugation)

Example: For $R = \mathbf{C}$ (complex numbers), define $\varphi : \mathbf{C} \to \mathbf{C}$ by

$$\varphi(a + bi) = a - bi \qquad \varphi(z) = \overline{z} \qquad (1)$$

for $a, b \in \mathbf{R}$. Then φ is a homomorphism (check) and $\varphi^{-1} = \varphi$, so φ is an isomorphism, and therefore, an automorphism of $\mathbf{C}$.

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

Usu: $\overline{a+bi} = a-bi$

Homom: $\overline{z+w} = \overline{z} + \overline{w}$ $\overline{zw} = (\overline{z})(\overline{w})$

So when we see field automorphisms in Ch. 8 when constructing better codes, it may help to think of them as complicated versions of complex conjugation (taking the bar of a complex number).

You may have seen this as "complex roots of a real polynomial come in pairs"?

Induced automorphism on polynomials

I.e.: What happens when you apply an automorphism to the *coefficients* of a polynomial and leave the x's alone.

Φ = capital φ

Example: R a ring, $\varphi : R \to R$ be an automorphism of R. Define a map $\Phi : R[x] \to R[x]$ by saying for $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$,

apply phi to coeffs of f

$$(\Phi(f))(x) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0). \qquad (2)$$

I.e., we get $(\Phi(f))(x)$ by applying φ to the *coefficients* of $f(x)$. Then Φ is an automorphism of $R[x]$, called the **automorphism of** $R[x]$ **induced by** φ.

Ie., automorphism of coefficient ring induces automorphism on polynomial ring.

Induced automorphism and roots of a polynomial

Theorem

Let R be a ring, let $\varphi : R \to R$ be an automorphism of R, and let $\Phi : R[x] \to R[x]$ be the corresponding induced automorphism. Then for $f(x) \in R[x]$ and $\alpha \in R$, if $f(\alpha) = 0$, then $(\Phi(f))(\varphi(\alpha)) = 0$.

Pf omitted.

I.e., an induced automorphism sends roots to roots.

Example: Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with **real** coefficients, and suppose α is a complex root of $f(x)$.

Take $R = \mathbb{C}$ (complex #s)

φ = conjugation.

Start: $f(\alpha) = 0$, apply Thm.

$\Phi(f)$ is f, apply φ to coeffs.

Coefficient of f are real, so not changed by taking complex conjugates. So Phi(f) is just f again.

Thm says that $\bar{\alpha}$ is a root of Phi(f)=f. I.e., since f is a polynomial with real coefficients:

$f(\bar{\alpha}) = 0$ as well.

In slogan form: The complex roots of a polynomial with real coeffs come in conjugate pairs, $\alpha, \bar{\alpha}$. $(a+bi, a-bi)$

We'll use this generalization: If coefficients of f(x) don't change when applying an automorphism phi, then the roots of f come in "phi orbits":

$\alpha, \varphi(\alpha), \varphi(\varphi(\alpha)), \varphi(\varphi(\varphi(\alpha))), \ldots$

In Ch 8, we'll only use finite rings, so this must circle back.

7.6: Finite fields

Q1: What are all possible finite fields like?
Q2: How do we do computations in a finite field?

Definition

The **order** of a field F is defined to be the number of elements in F; a **finite field** is therefore the same as a field of finite order.

Definition

Ex of a finite field: F_p = Z/(p), p prime.

Let R be a ring. Since R has a multiplicative identity 1, for a positive integer n, we can abbreviate

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}. \tag{3}$$

Then define $\mathrm{char}(R)$, the **characteristic** of R, by: (Add 1 to itself repeatedly, see what happens)

- If $n \cdot 1 = 0$ for some positive integer n, then $\mathrm{char}(R)$ is smallest positive n such that $n \cdot 1 = 0$.
- If $n \cdot 1 \neq 0$ for all positive integers n, then $\mathrm{char}(R) = 0$.

Ex. $\mathrm{char}(\mathbb{Z}) = 0$

Think: For $R = \mathbf{Z}/(m)$, $\mathrm{char}(R) = m$. But also $\mathrm{char}(\mathbf{F}_p[x]) = p$ (e.g., we always have $2 = 0$ in $\mathbf{F}_2[x]$).

Example: If f(x) is a polynomial in F_2[x], then

$$f(x) + f(x) = (a_n x^n + \cdots + a_0) + (a_n x^n + \cdots + a_0)$$

$$= 2a_n x^n + \cdots + 2a_0$$

$$= 0x^n + \cdots + 0$$

$$= 0.$$

Char(R) = 2 means that 2 = 0, even though we have a lot more elements in the ring than we have in Z/(2).

Characteristic of a finite field

Theorem So every finite field is based on F_p for some prime p.

Let F be a finite field. Then $\mathrm{char}(F) = p$ *for some prime* p.

Proof: Could we have $\mathrm{char}(F) = 0$?

In that case, we would have 1, 1+1, 1+1+1, etc. are all different elements, so F would have to contain infinitely many different elements -- not possible b/c F is finite.

Could we have $\mathrm{char}(F) = ab,\ a, b > 1$?

zero divisors

In that case, we would have (a*1)(b*1) = (ab*1) = 0, but (a*1), (b*1) not equal to 0.

That would mean that F would contain zero divisors, which can't happen in a field.

$\mathbb{Z}/(p)$

Punchline: Any finite field K has a copy of $\mathbf{F}_p$ (p prime) sitting inside it; we'll see how to construct K starting with that $\mathbf{F}_p$.

The multiplicative group of a finite field

Definition

Let F be a field. We use $F^\times$ to denote the set of all nonzero elements of F, all of which are units (since F is a field). We therefore call $F^\times$ the **multiplicative group** of F.

Definition

for now, "group" is not yet defined; could just think "set"

Let $F^\times$ be the multiplicative group of the field F, and suppose $\alpha \in F^\times$. We define the **cyclic subgroup generated by** α to be the set $\langle \alpha \rangle = \{\alpha^n \mid n \in \mathbf{Z}\}$, or in other words, the set of all powers of α, positive, negative, or zero.

not yet defined

Definition

Let $F^\times$ be the multiplicative group of the field F, ~~and suppose $\alpha \in F^\times$~~. To say that $F^\times$ is **cyclic** means that there exists some $\alpha \in F^\times$ such that $F^\times = \langle \alpha \rangle$, or in other words, such that every element of $F^\times$ is some power of α. If $F^\times = \langle \alpha \rangle$, we say that α is a **primitive** element of F.

Every finite field has a primitive element

(Fact ¡pf beyond our course)

Theorem

If F is a finite field, then its multiplicative group $F^\times$ is cyclic. In other words, every finite field contains a primitve element.

We saw this in practice before with $\mathbf{F}_p$: If you look for long enough in $\mathbf{Z}/(p)$, you run into a primitive element (in fact usually lots).

ie, element whose powers eventually hit every nonzero element of F_p

Oders of (primitive) elements

Definition

Let $F^\times$ be the multiplicative group of the field F, and suppose $\alpha \in F^\times$. If $\alpha^n = 1$ for some positive integer n, we define the **order** of α to be the *smallest* possible n such that $\alpha^n = 1$. Otherwise, if $\alpha^n \neq 1$ for all positive integers n, we say that α has **infinite order**.

Theorem

Let F be a field of order n, let $F^\times$ be the multiplicative group of F, and suppose $\alpha \in F^\times$. Then:

1. *The order of α is equal to the order of (number of elements in) $\langle \alpha \rangle$. It follows that α is primitive if and only if the order of α is equal to $n-1$, the order of $F^\times$.*
2. *If k is the order of α, then the order of α^m is $\dfrac{k}{\gcd(k,m)}$.*
3. *If k is the order of α, then k divides $n-1$ (the order of $F^\times$).*

Example: $\mathbf{F}_{11} = \mathbf{Z}/(11)$ $q = 11$

Problem: Find a primitive element in $\mathbf{F}_{11}$ and find the orders of all elements of $F_{11}^{\times}$.

Thm 1. primitive elt has order 10.

Thm 3. Any elt has order 1, 2, 5, or 10.

So: If we take powers of an element and don't get 1 by the 5th power, elt must be primitive.

Example: Is 2 a primitive element of F_11?

order is not 2

mod 11

$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10$

We see order of 2 is >5, so must be 10 (by Thm).
So 2 is a primitive element of F_11.

The magic polynomial

Corollary

Let F be a field of order q. Then every α is a root of the polynomial $x^q - x \in F[x]$, and consequently,

$$x^q - x = \prod_{\alpha \in F} (x - \alpha). \tag{4}$$

Example: For $\mathbf{F}_{11} = \mathbf{Z}/(11)$, this means:

Proof: (Assuming previously stated facts about orders)

Deeper stuff about finite fields

You just have to know these facts; don't worry about their proofs:

Theorem

Let F be a finite field of characteristic p. Then F is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x) \in \mathbf{F}_p[x]$.

Theorem

Let p be a prime, and let e be a positive integer.

1. *There exists at least one field of order p^e.*
2. *If F and K are both finite fields of order p^e, then F and K are isomorphic.*

Definition

Since any two fields of order p^e are isomorphic, algebraically we can think of them as being the same. For $q = p^e$ (p prime, $e \geq 1$), we may therefore define $\mathbf{F}_q$ to be "the" field of order q. This field is also sometimes known as the **Galois field of order** q, or $GF(q)$ for short.

Recap: Five Facts For Finite Fields

1. The characteristic of a finite field must be a prime p, and its order must be $q = p^e$ for some $e \geq 1$.
2. Every finite field has a primitive element.
3. If F is a field of order q, then every $\alpha \in F$ is a root of $x^q - x$, or in other words, $\alpha^q = \alpha$ for every $\alpha \in F$. Consequently, $x^q - x$ factors as the product of all $(x - \beta)$, where β runs over all elements of F (including $0 \in F$).
4. Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$.
5. For any prime p and $q = p^e$ $(e \geq 1)$, there exists a field $\mathbf{F}_q$ of order q that is unique up to isomorphism.