Math 127, Mon Apr 12

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 7.6–7.7. Reading for Wed: 8.1–8.2 (**reload book**). Brand new!
- PS07 due tonight; PS08 outline due Wed night.
- Problem session Fri Apr 16, 10am–noon.

Computation in $F[x]/(m(x))$, α notation $= F[\alpha]$

F a field, $m(x) \in F[x]$ ($\deg m = k > 0$), $I = (m(x))$ (the polynomial multiples of $m(x)$). Abbreviate $\alpha = x + I$. Working mod I, we have: Think: F[x]/(m(x)) is just like Z/(m).

- **Elements:** The cosets of I in $F[x]$, which we can write as $r(\alpha)$ where $\boxed{\deg r < k}$, since setting $m(\alpha) = 0$ allows you to reduce any polynomial of degree $\geq k$.
  More specifically, if $\deg m = k$, then you rewrite $m(\alpha) = 0$ as a **reduction relation** $\alpha^k = \cdots$ and apply that repeatedly to reduce any higher-degree terms to terms of degree $< k$.

  like 0,...,m-1 in Z/(m)

- **Operations:** Addition and multiplication are computed in polynomials in α and then reduced. I.e., you use the relation $m(\alpha) = 0$ to choose a **reduced representative** for the final answer.

Reciprocal of $b(\alpha)$ by computing $\gcd(b(x), m(x))$ and Euclidean Reduction for polynomials.

Cor: $\overline{R}$ is a field if and only if $m(x)$ is irreducible.

$R =$ F[x]/(m(x))

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 $r, s \in R$,

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

In other words, a homomorphism is a function between rings that preserves addition and multiplication.

Definition

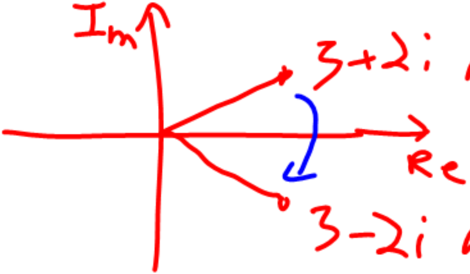
An **isomorphism** is a bijective (one-to-one and onto) homomorphism. To say that rings R and R' are **isomorphic** means that there exists some isomorphism $\varphi : R \to R'$.

One point of isomorphisms: When two rings R and R' are isomorphic, they're really the same ring, using different names. In particular, they have the same abstract properties (units, zero divisors, principal ideals, etc.).

Recap of complex conjugation

$$\varphi(a+bi) = a-bi$$

$$\overline{3+2i} = 3-2i$$



$3+2i$ at $(3,2)$

$3-2i$ at $(3,-2)$

Automorphisms

Another reason to be interested in isomorphisms:
Defn: An **automorphism** is an isomorphism $\varphi : R \to R$ from a ring to itself. Interesting b/c phi reveals a symmetry of the ring R.

Exmp: Let $\varphi : \mathbf{C} \to \mathbf{C}$ be $\varphi(a + bi) = a - bi$ for $a, b \in \mathbf{R}$. Then φ is a homomorphism (PS08) and $\varphi \circ \varphi$ is the identity, so φ is a bijective homomorphism and therefore an automorphism of $\mathbf{C}$.
Exmp: Let R be a ring, and let $\varphi : R \to R$ be an automorphism of R. Define a map $\Phi : R[x] \to R[x]$ by

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

Φ capital version of phi

In other words, $(\Phi(f))(x)$ is obtained 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. Think: Applying complex conjugation to coefficients of a polynomial.

Symmetries of the 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 $(\Phi(f))(\varphi(\alpha)) = 0$.

Special case/the point: Let $f(x) \in \mathbf{R}[x]$ be a polynomial with *real* coefficients. If $a + bi$ is a *complex* root of $f(x)$, then because the automorphism of complex conjugation leaves f unchanged ("invariant"), $a - bi$ is also a root of $f(x)$. (In other words, non-real roots of real polynomials come in conjugate pairs.)

Example: Consider $f(x) = x^4 + 5x^2 + 4$. $= (x^2+1)(x^2+4)$

φ conj. $\Phi(f(x)) = f(x)$

So: If $a+bi$ is root of f, so is

$a-bi$.

$x^2+4=0$ $x^2+1=0$

$f(x)=x^4+5x^2+4=(x^2+4)(x^2+1)$

Roots of f: $+2i, -2i, +i, -i$

So again, here, if (a+bi) is a root of f, so is its complex conjugate a-bi.
More generally, if alpha is a root of f, and phi is an automorphism of C that fixes the coefficients of f, then phi(alpha) is also a root of f.

Order and characteristic

$\boxed{m(x)\ \text{irr.}}$

Ex $\mathbb{F}_p[x]/(m(x))$

Definition

The **order** of a field F is defined to be the number of elements in F; i.e., **finite field** is a field of finite order.

Ex $\mathbb{Z}/(p) = \mathbb{F}_p$

Definition

Let R be a ring. Abbreviate $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}$. Then either:

1. $n \cdot 1 = 0$ for some positive integer n; or $\mathbb{Z}/(m)$
2. $n \cdot 1 \neq 0$ for all positive integers n. $\mathbb{Z}$

In case (1), char(R) is the smallest positive integer n such that $n \cdot 1 = 0$; and in case (2), char$(R) = 0$. char(R) = characteristic of R

Exmp: For $R = \mathbf{Z}/(m)$, char$(R) = m$.

Exmp: $\mathbf{F}_p[x]$ has characteristic p, and if $m(x) \in F_p[x]$ has $\deg(m(x)) \geq 1$ then $\mathbf{F}_p[x]/(m(x))$ also has characteristic p.

Point:

While F_p[x] has infinitely many elements, the coefficients are still all mod p, so F_p has characteristic p. I.e., still true that p = 0.

Question: What do all finite fields look like?

Answer: They all look like F_p[x]/(m(x)).

Characteristic of a finite field

So $\{0, 1, \dots, p-1\}$ in F

Theorem

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

Point: If F is a finite field, then F has a copy of some $\mathbf{Z}/(p) = \mathbf{F}_p$ sitting inside it. We can think of this copy of $\mathbf{F}_p$ as a base on which F is constructed.

Why:

Because F has finitely many elements, if we do 1+1+1+..., we eventually hit 0, so F must have characteristic n for some n>0.

If n = ab, 1<a,b<n, then from the distributive law, we get (eventually)

(a*1)(b*1)
= (1+...+1) (1+...+1)

a times b times

= (ab*1) = n*1 = 0. So F would have zero divisors, which a field can't have.

Even more vocabulary

Definition

Let F be a field. We use $F^\times$ to denote the set of all nonzero elements of F, and call $F^\times$ the **multiplicative group** of F.

Groups are objects to be introduced later.

Definition

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 $\langle\alpha\rangle = \{\alpha^n \mid n \in \mathbf{Z}\}$, i.e., the set of all powers of α, positive, negative, or zero.

Definition

To say that $F^\times$ is **cyclic** means that there exists some $\alpha \in F^\times$ such that $F^\times = \langle\alpha\rangle$, i.e., 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.

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.

Alas, a different definition of order

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 $F^\times$).*

Remember, there are two important definitions of the word "order":

* The order of a set of things (e.g., a field, the cyclic subgroup generated by alpha) is the number of things in that set, i.e., its size.

* The (multiplicative) order of an element alpha is the smallest power n of alpha such that alpha^n = 1.

Confusing! But Statement 1 of the above theorem shows that these two meanings agree when they both occur, at least?

¯_(ツ)_/¯

Example: Some orders of elements in $\mathbf{F}_{17} = \mathbb{Z}/(17)$

order(2)?

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 = -1$

$2^5 = 2^4 \cdot 2 = -2,\ 2^6 = -4,\ 2^7 = -8$

$2^8 = 1$ $\boxed{\text{order}(2) = 8}$

$\mathbb{F}_{17} = \{0, 1, \ldots, 16\}$

$\mathbb{F}_{17}^\times = \{1, \ldots, 16\}$

size of $\mathbb{F}_{17}^{\times} = |\mathbb{F}_{17}^{\times}| = 16$

In general, for a field of order q, the multiplicative group has order q-1.
So part 3 of the Theorem says that order of any element of mult group of F_{17} has order dividing 16.

$\boxed{\mathbb{F}_{17}}$

Order(3)? $= 1, 2, 4, 8$, or 16.

$3^1 = 3, 3^2 = 9,$

$3^4 = (3^2)^2 = 81 \equiv 13 \equiv -4 \pmod{17}$

$3^8 = (3^4)^2 = 16 \neq 1$

So $\operatorname{order}(3) \neq 1, 2, 4, 8$

$\Rightarrow \operatorname{order}(3) = 16$

$\Rightarrow \langle 3 \rangle = \{ \ldots, 3^{-2}, 3^{-1}, 3^{0}, 3^{1}, 3^{2}, \ldots \}$

$= \mathbb{F}_{17}^{\times}$ i.e. 3 is prim

Next! Powers of 3 in order

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,

$$x^q - x = \prod_{\alpha \in F} (x - \alpha). \tag{1}$$

Proof:

Deeper facts about finite fields

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 $m(x) \in \mathbf{F}_p[x]$.

So the order of a finite field must be p^e for some prime p and some positive integer e. More surprisingly:

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*

I.e., for any prime p and some positive integer e, there is only one field of order $q = p^e$.

Five Facts for Finite Fields

1. **Prime power:** 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. **Orders of elements:** The multiplicative group of a finite field is cyclic; i.e., if F has q elements, $F^\times$ must contain at least one element of order $q - 1$. Moreover, every element of $F^\times$ must have order dividing $q - 1$.
3. **Magic polynomial:** 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.
4. **Construction:** Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$.
5. **Classification:** 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.

Example: One approach to the field of order 8

Construction, magic polynomial, orders of elements: