Math 127, Mon Apr 11

Back Mon Apr 18!

- Reading for today: 7.4–7.6.
- Reading for Mon Apr 18: 8.1–8.2.
- PS08 outline due tomorrow(-ish) and completed version due Tue(-ish).

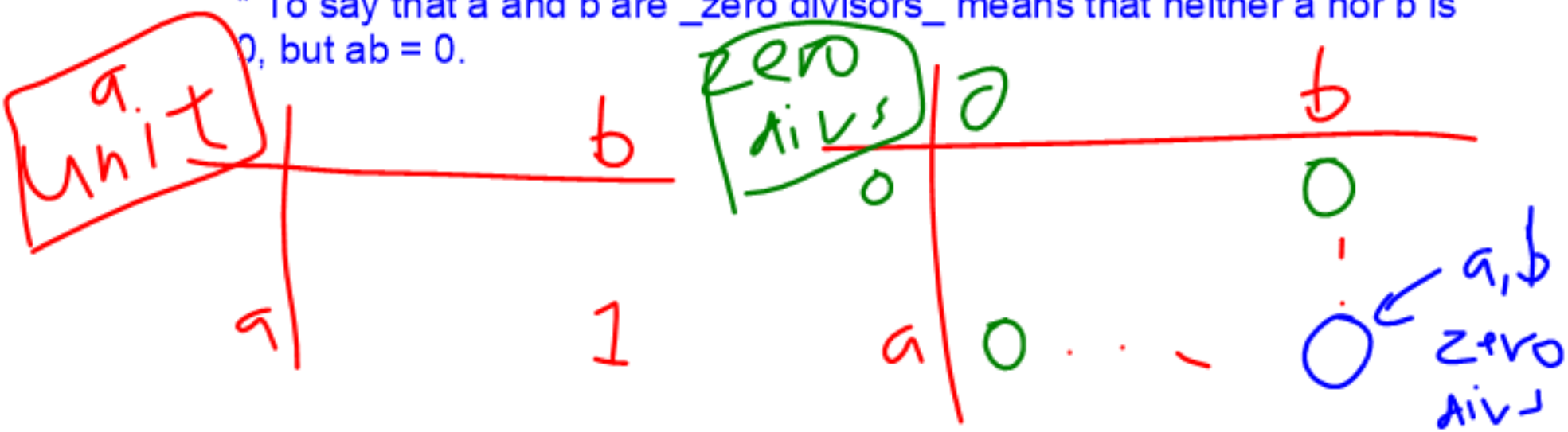
** Problem session and checkin on Fri Apr 15, 10am-noon

7.3.4 (p507)

$R_1 = F_2[x]/(x^2+1)$ | $R_2 = F_2[x]/(x^4+x+1)$

(g) In a ring R, a and b in R:

* To say that a is a _unit_ means that there is some b in R such that ab=1.
* To say that a and b are _zero divisors_ means that neither a nor b is 0, but ab = 0.



Principal ideal domains

To say that a ring R is a **principal ideal domain**, or **PID**, means that R is an integral domain and that every ideal of R is principal. In other words, the second condition says that if I is an ideal of R, then $I = (a)$ (the set of all R-multiples of a) for some $a \in I$.

Theorem

Let R be either $\mathbf{Z}$ or $F[x]$ (F a field), or more generally, let R be a Euclidean domain. Then R is a PID.

Proof, case $R = \mathbf{Z}$: We apply signed division:

If $a, d \in \mathbf{Z}$, $d \neq 0$, then for some $q, r \in \mathbf{Z}$,

$$a = dq + r \qquad \text{with } |r| \leq \frac{|d|}{2}.$$

Proof that Z is a PID:

(what makes a polynomial "small"?)

Suppose I is an ideal of Z (= the integers).
If I = {0} then I = (0); otherwise, I contains nonzero elements.

Choose some nonzero d in I such that |d| is as small as possible among all nonzero elements of I.

Suppose a is some element of I. Our goal now is to show that a is a multiple of d; that will prove that I = (d).

Apply signed division to divide a by d, and we get:

$a = dq + r$ $\longrightarrow$ $|r| \leq \frac{|d|}{2}$

So r = a - dq.

Because d in I and I is an ideal, dq is in I.
Because a in I and dq in I and I is an ideal, a - dq is in I.

So r is in I, and r has smaller absolute value than d.
Since d has smallest possible absolute value among nonzero elements of I, r has to be equal to 0. So a = dq, which is what we WTS.

What kind of division will we be using here?

The minimal polynomial

To recap: We know in the abstract that if I is an ideal of $F[x]$, then there is some $d(x)$ such that $I = (d(x))$. If we choose $d(x)$ to be **monic** (leading coefficient 1), then we call $d(x)$ the **minimal polynomial** of I.

Note that we only know $d(x)$ exists in the abstract, and in practice, we use different methods to figure out what $d(x)$ is in different circumstances.

End 7.4

Homomorphisms

7.5

A thing that looks abstract but is fundamental. (And is surprisingly useful!)

dom

codomain

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.

Example: Substitution homomorphism

Let F be a field, and fix some $\alpha \in F$. We define a function $\varphi : F[x] \to F$ by declaring

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

phi means "plug in alpha for x"

for all $f(x) \in F[x]$. Then φ turns out to be a type of homomorphism known as a **substitution homomorphism**. What does φ (substitution) being a homomorphism mean in practice?

$f, g \in F[x]$ φ hom means

$\varphi(f(x)+g(x)) = \varphi(f(x)) + \varphi(g(x))$

add f, g first, then plug α

plug α into f, g then add results

phi being a homomorphism means that whether you add polynomials and then plug in alpha, or plug in alpha and then add the results, you get the same answer.

phi being a homomorphism also means that the same thing holds for multiplication.

Non-hom def $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$

$\varphi(f(x)) = f(x)^2$

φ is not a hom b/c: $f(x) = x^2$, $g(x) = x^2$

$\varphi(f(x) + g(x)) = \varphi(x^2 + x^2) = \varphi(2x^2) = 4x^4$

$\varphi(f(x)) + \varphi(g(x)) = \varphi(x^2) + \varphi(x^2) = x^4 + x^4 = 2x^4$

OTOH: If coefficients are in F_2, then the same phi *is* a homomorphism! PS08.

When are two rings "the same"?

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 $\varphi : R \to R'$.

Suppose $\varphi : R \to R'$ is an isomorphism. Then:

- The elements of R and the elements of R' are paired up bijectively (one-to-one correspondence).
- This pairing (given by φ) preserves the operations $+$ and $\times$.
- Conclusion: R and R' are really the "same" ring, but with different names for the elements.

Properties preserved under isomorphism

If R and R' are isomorphic rings, we have that, for example:

- R and R' have the same number of units.
- R is an integral domain if and only if R' is an integral domain.
- R is a field if and only if R' is a field.
- R is a PID if and only if R' is a PID.

That is, any property of a ring that can be defined abstractly, based on the axioms of a ring, is preserved under isomorphism. On the other hand, if R and R' don't share a particular abstract property, then R and R' can't be isomorphic.

Example: Suppose R is a ring that is not a field (i.e., R has nonzero elements that do not have inverses). Then any field F can't be isomorphic to R.

Automorphisms

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

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 and $\varphi \circ \varphi$ is the identity, so φ is an isomorphism, 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

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

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.

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

i.e. $\varphi(z) = \overline{z}$ ← complex conjugation

φ hom. For $a+bi, c+di \in \mathbb{C}$.

Check

$$\varphi((a+bi)(c+di)) = \varphi(a+bi)\varphi(c+di)$$

Multiply, then take complex conjugate

Take complex conjugates, then multiply

And similarly for addition, so phi is a homomorphism.

Symmetries of the roots of a polynomial

and $\Phi(f) = f$, i.e., phi fixes every coefficient of f

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 $(\Phi(f))(\varphi(\alpha)) = 0$. i.e., phi(alpha) is also a root of f.

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 $a - bi$ is also a root of $f(x)$. (In other words, non-real roots of real polynomials come in conjugate pairs.)

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

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

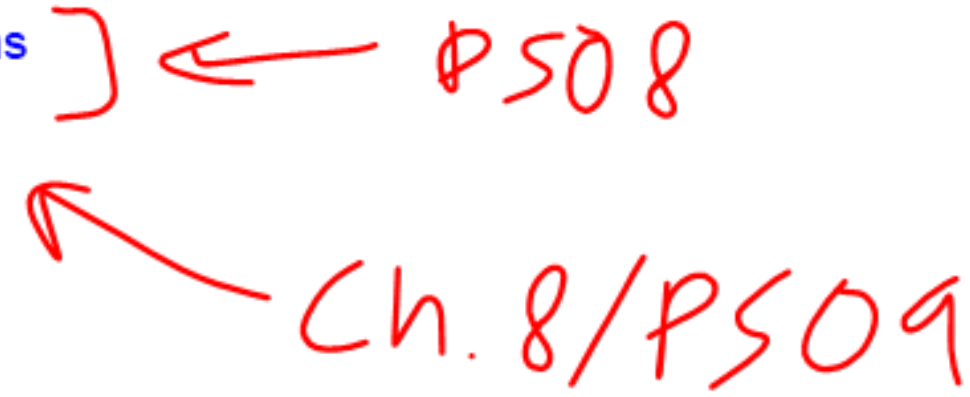
Roots of f: $2i, -2i; i, -i$

Something like this will play a key role in constructing better error-correcting codes.

Any questions for now about:

* homomorphisms
* isomorphisms
* automorphisms

?



Order and characteristic

7.6

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.

e.g. $\mathbb{Z}/(3) = \{0, 1, 2\}$

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
2. $n \cdot 1 \neq 0$ for all positive integers n.

the characteristic of R

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

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

Characteristic of a finite field

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: By Pigeonhole, eventually $n \cdot 1 = m \cdot 1$ $(m > n)$

$\Rightarrow (m-n) \cdot 1 = 0$ So $\mathrm{char}(F) \neq 0$.

If $\mathrm{char}(F) = m = ab$ $a, b \neq 1$,

then $(a \cdot 1)(b \cdot 1) = m \cdot 1 = 0$

So F has zero divs $a \cdot 1, b \cdot 1$;
CONTRA.

So $\mathrm{char}(F)$ must be prime.

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.

all units

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.

OK b/c α^{-1} exists.

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 $F^\times$).*

Example: Some orders of elements in $\mathbf{F}_{17}$

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,

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

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.