Math 128B, Wed Mar 17

- 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: Ch. 20.
- PS06 outline due Wed night, full version due Mon.
- Problem session Fri Mar 19, 10am–noon.
- **Exam 2 in one week**, on Chs. 15–19 (PS04–06). Review session Mon night (recorded to YouTube).

Recap of vector spaces

(V,+) ab gp; a(v+w)=av+aw, (a+b)v = av + bv;
(ab)v=a(bv), 1v=v.

- Anything that satisfies the axioms is a vector space over F.
- Primary case: An extension field of F is a vector space over F.
- If a vector space has a finite basis, then its dimension is well-defined.
- A maximal linearly independent set is a basis (PS06).
- A finite field of characteristic p has $\mathbf{Z}_p$ as a subfield, so is a vector space over $\mathbf{Z}_p$.
- Other extension fields we'll study will be finite-dimensional by construction or by assumption.

(Ch 13): If R ring with 1, char(R) = # of times add 1 to itself to get 0.
char(R) = 0 means that you never get 0 when add 1 to itself.

Thm: Any field has characteristic 0 or characteristic p (p prime).

Extension fields and how to construct them

Definition

To say that E is an **extension field** of F means that E is a field and F is a subfield of E.

Theorem

F a field, $f(x) \in F[x]$, $\deg f > 0$. Then there exists an extension field E of F such that f has a zero in E. Specifically, if $p(x)$ is irreducible, then p has a zero in $F[x]/\langle p(x) \rangle$.

Proof when $p(x)$ irreducible: Let $I = \langle p(x) \rangle$ and let $\alpha = x + I \in F[x]/I$. Because p(x) irreducible, E = F[x]/I is a field.

Let phi: F[x] -> F[x]/I be the natural homomorphism.
Because the intersection of F and ker(phi) is 0, phi is injective on F.
So we can think of F as a subfield of E.
So we can think of p(x) as a polynomial in E[x].

So $p(x) = c_n x^n + \cdots + c_0$

$$
\begin{aligned}
p(\alpha) &= c_n \alpha^n + \cdots + c_1 \alpha + c_0 \\
&= c_n (x+I)^n + \cdots + c_1 (x+I) + c_0 \\
&= (c_n x^n + I) + \cdots + (c_1 x + I) + c_0 \\
&= c_n x^n + \cdots + c_1 x + c_0 + I \\
&= p(x) + I = p(x) + \langle p(x) \rangle \\
&= 0 + \langle p(x) \rangle,
\end{aligned}
$$

which is the zero element of E.

Recap/clarification/computation

Suppose $p(x)$ irreducible in $F[x]$, $\deg p = n > 1$. Let $I = \langle p(x) \rangle$.
How can we compute in $F[x]/I$? = E, ext of F

By Division Thm, if we divide $f(x) \in F[x]$, there exists **unique** $q, r \in F[x]$ such that $f(x) = q(x)p(x) + r(x)$ and $\deg r < \deg p$. Follows that every element of $F[x]/I$ can be expressed uniquely in the form $r(x) + I$ with $\deg r < \deg p$.

by p

So if we let $\alpha = x + I$, then every element of $F[x]/I$ can be expressed uniquely in the form $r(\alpha)$ with $\deg r < \deg p$. We may therefore write $F(\alpha) = F[x]/I$ and say that $F(\alpha)$ is F, adjoining a root of $p(x)$.

α

Note: $F(\alpha)$ is a v.s. over F, and since any element of $F(\alpha)$ can be written uniquely in the form $c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$, $\{\alpha^{n-1}, \ldots, \alpha, 1\}$ is a basis for $F(\alpha)$, and $\dim F(\alpha) = n = \deg p$.

A finite example

How can you compute in $\mathbf{Z}_2(\alpha)$, where α is a root of $x^4 + x + 1$? $\in \mathbb{Z}_2[x]$

$$\left(\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[x] / \langle x^4 + x + 1 \rangle \right)$$

What is $\mathbb{Z}_2(\alpha)$?

Elts "Polys in α" of deg ≤ 3:

$c_3\alpha^3 + c_2\alpha^2 + c_1\alpha + c_0 \qquad c_3, c_2, c_1, c_0 \in \mathbb{Z}_2$

Defining rel'n of $\mathbb{Z}_2(\alpha)$:

$\alpha^4 + \alpha + 1 = 0$

So $\alpha^4 = -\alpha - 1 = \alpha + 1$ $\left(\begin{array}{c}+1=-1\\ \text{in } \mathbb{Z}_2\end{array}\right)$

and can reduce any poly deg > 3

by repeating $\alpha^4 = \alpha + 1$.

<u>Dimension</u>: $\{\alpha^3, \alpha^2, \alpha, 1\}$ is a basis for $\mathbb{Z}_2(\alpha)$ over $\mathbb{Z}_2$.

So $\dim(\mathbb{Z}_2(\alpha)) = 4$.

$$GF(16) = \mathbb{Z}_2(\alpha)$$

(There are $2^4 = 16$ elts of $\mathbb{Z}_2(\alpha)$.)

Splitting fields

E an extension field of F, $a_i \in E$.

(intersection of all possible)

Definition

$F(a_1, \ldots, a_k)$ is the smallest subfield of E containing $a_1, \ldots, a_k$.
Think: $F(a_1, \ldots, a_k)$ is the **field** generated by F and $a_1, \ldots, a_k$.

I.e., smallest subset of E containing F, a_1,...,a_k that is closed under +, -, mult, division.

Definition

$f(x) \in F[x]$, $\deg f = k > 0$.

- To say f **splits** in E means that

$$f(x) = a(x - a_1) \cdots (x - a_k)$$

  for some a $a_1, \ldots, a_k \in E$.
- If also $E = F(a_1, \ldots, a_k)$, we say that E is a **splitting field for f over F**.

E generated by F and roots of f

Examples

- $\mathbf{C}$ is a splitting field of $x^2+1=(x+i)(x-i)$ over $\mathbf{R}$.
- $\mathbf{Q}(i)=\{a+bi \mid a,b\in\mathbf{Q}\}$ is a splitting field of $x^2+1=(x+i)(x-i)$ over $\mathbf{Q}$.
- $\mathbf{Z}_3(i)=\{a+bi \mid a,b\in\mathbf{Z}_3\}$ is a splitting field of $x^2+1=(x+i)(x-i)$ over $\cancel{\mathbf{Q}}$ $\mathbf{Z}_3$
- $\mathbf{Z}_2$ is a splitting field of $x^2+1=(x+1)^2$ over $\mathbf{Z}_2$.

Goal for rest of today: Show that we can replace each "a splitting field" with "**the** splitting field."

I.e., we will show that every polynomial in $F[x]$ has a splitting field in $F[x]$, and that any two splitting fields of $f(x)$ over F are isomorphic.

next

Non-example $\alpha = \sqrt[3]{5}$

$\mathbb{Q}(\alpha) = E$, ext of $\mathbb{Q}$.

Turns out:

$$x^3 - 5 = x^3 - \alpha^3$$

$$= (x-\alpha)\underbrace{(x^2+\alpha x+\alpha^2)}_{\text{irr over } E}$$

$\sqrt{\alpha^2 - 4\alpha^2} \notin \mathbb{R}$

So $x^3 - 5$ doesn't split over E.

Splitting field is ext of E ....

Why do we care about splitting fields?

The basic question of the entire semester is:

$$\textit{Solve } f(x) = a_n x^n + \cdots + a_1 x + a_0 = 0 \textit{ over } F.$$

IDEA: Instead of looking at the (finite) solution set $a_1, \ldots, a_k$ to $f(x) = 0$, study the splitting field $F(a_1, \ldots, a_k)$.

We can use then algebraic structures like fields, vector spaces (!), and finite nonabelian groups (!?!) to learn more about $F(a_1, \ldots, a_k)$, and therefore, about $a_1, \ldots, a_k$.

Existence of splitting fields

Theorem
$f(x) \in F[x]$, $\deg f > 0$. *Then there exists a splitting field* E *for* $f(x)$ *over* F*.*

Why:

Adjoining one root

Theorem

F a field, $p(x) \in F[x]$ irreducible over F. If E an extension of F, $a \in E$, and $p(a) = 0$, then

$$F(a) \approx F[x]/\langle p(x)\rangle \,.$$

Claim 1: Kernel of substitution homomorphism $\varphi : F[x] \to F(a)$ given by $\varphi(f(x)) = f(a)$ is:

Claim 2: Image of φ is:

Uniqueness of splitting fields

From previous result:

Corollary

$p(x) \in F[x]$ irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then $F(a) \approx F[x]/\langle p(x)\rangle \approx F(b)$.

Long story short, carefully applying the above corollary and induction gives:

Corollary

Any two splitting fields of $f(x) \in F[x]$ are isomorphic.

Roots of unity

Picture of the nth roots of unity in the complex plane:

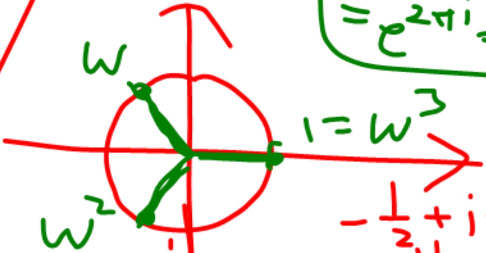
$n = 5$

$\omega = e^{\frac{2\pi i}{5}}$

$\omega = e^{\frac{2\pi i}{n}}$

$\omega^n = \left(e^{\frac{2\pi i}{n}}\right)^n = e^{2\pi i} = 1$

$n = 3$



$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$\omega = e^{\frac{2\pi i}{3}} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

Example: The splitting field of $x^3 - 7$

Generators, basis, dimension:

$\alpha = \sqrt[3]{7}$, $w = e^{\frac{2\pi i}{3}}$

$p(x) = x^3 - 7 = (x-\alpha)(x^2 + \alpha x + \alpha^2)$

$= (x-\alpha)(x - w\alpha)(x - w^2\alpha)$

Split of $x^3 - 7$ is $\mathbb{Q}(\alpha, w) = K$

$\to$ p splits over K

$\to$ Field gen'd by $\alpha, w\alpha, w^2\alpha$

contains α, $\frac{w\alpha}{\alpha} = w \Rightarrow K$.