Lecture 25: Finite fields

Monday, June 4, 2018 11:18 AM

In the previous lecture we proved:

Theorem. If $f(x)\in\mathbb{Z}_p[x]$ is irreducible of degree n, then $E:=\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field of order p^n.

An important property of a finite field of order p^n is the following:

Lemma. Suppose E is a field and $|E|=q$. Then

$$\forall \alpha\in E,\quad \alpha^q=\alpha.$$

Pf. If $\alpha=0$, then $\alpha^q=0=\alpha$. If $\alpha\neq 0$, then $\alpha\in U(E)$. By Lagrange's theorem $\alpha^{|U(E)|}=1$; and so $\alpha^{q-1}=1 \Rightarrow \alpha^q=\alpha$. ■

Theorem. Suppose E is a finite field and $|E|=q$. Then

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

Pf. By the previous lemma, $\forall\alpha\in E$ is a zero of x^q-x. And so $\exists\, g(x)\in E[x]$, $x^q-x=g(x)\prod_{\alpha\in E}(x-\alpha)$.

Comparing degrees we get $q=\deg g+|E|=\deg g+q$.

Lecture 25: A splitting field of a polynomial

Friday, June 1, 2018 11:40 AM

And so $\deg g = 0$. This means $g(x) = c \in E \setminus \{0\}$.

Comparing the leading coeff. we deduce that $c = 1$ and claim follows. ■

We will come back to this theorem later. For now let's go back to zeros of polynomials. So far we have found a field extension that contains a zero of an irreducible polynomial. Can we find a field extension that contains all the zeros of an arbitrary positive degree polynomial?

Def. Suppose F is a field, $f(x) \in F[x]$ has positive degree; E is called a splitting field of f over F if

(1) $F \overset{i}{\hookrightarrow} E$; that means i is an injective ring homomorphism.

(2) $\exists\, \alpha_1, \ldots, \alpha_n \in E$, $f(x) = c\,(x-\alpha_1) \cdots (x-\alpha_n)$
$c \in E$

(3) E is the smallest field that contains $i(F)$ and $\alpha_1, \ldots, \alpha_n$.

Lecture 25: Examples of splitting fields

Monday, June 4, 2018 2:25 PM

Ex. $\mathbb{Q}[\sqrt{2}]$ is a splitting field of x^2-2 over $\mathbb{Q}$.

Solution. $\cdot$ $\mathbb{Q} \hookrightarrow \mathbb{Q}[\sqrt{2}]$

$a \longmapsto a$

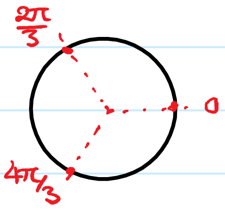
$\cdot$ $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$

$\cdot$ If a ring contains $\mathbb{Q}$ as a subring and $\sqrt{2}$, then $\forall a,b\in\mathbb{Q}$, $a+b\sqrt{2}$ is in that ring. Hence $\mathbb{Q}[\sqrt{2}]$ is the smallest subring of $\mathbb{Q}[\sqrt{2}]$ that contains $\mathbb{Q}$ and $\sqrt{2}$.

Ex. Find a splitting field of x^3-2 over $\mathbb{Q}$.

Solution. A splitting field E of x^3-2 over $\mathbb{Q}$ contains zeros of x^3-2. Let's start with finding zeros of this polynomial in $\mathbb{C}$.

If a complex number z is a zero of x^3-2, then $z^3=2$. Using polar coordinates and Euler formula, we have $z=re^{i\theta}$ where $r=|z|$ and $\theta=\arg(z)$. Hence $(re^{i\theta})^3=2$ implies $r^3=2$ and $e^{3i\theta}=1$. And so $r=\sqrt[3]{2}$ and $3\theta=2k\pi$ for some $k\in\mathbb{Z}$. Hence

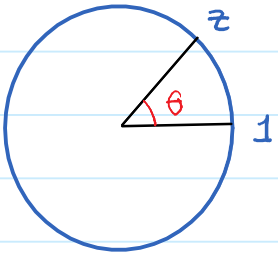


Lecture 25: Examples of splitting fields

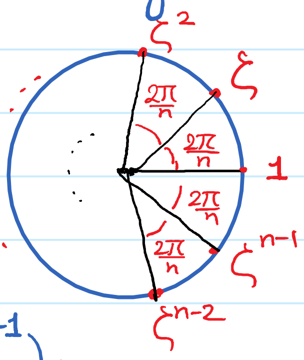
Monday, June 4, 2018 2:38 PM

[Recall from complex numbers:

if $z\in\mathbb{C}$ and $z^n=1$, then $|z|^n=1$ implies $|z|=1$. And so z is on the unit circle. If the argument of z is θ, then multip. by z is just rotation by angle θ about the origin. So $z^n=1$ means after $\underline{n}$ times rotation we get back to 1. Therefore $n\theta=2k\pi$ for some $k\in\mathbb{Z}$. Hence we get n possible values $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ where



$$\zeta = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\,\sin\left(\frac{2\pi}{n}\right).$$



And so $y^n-1=(y-1)(y-\zeta)\cdots\cdots(y-\zeta^{n-1})$.]

Hence $\sqrt[3]{2}, \sqrt[3]{2}\,\zeta, \sqrt[3]{2}\,\zeta^2$ are zeros of x^3-2 where $\zeta=e^{\frac{2\pi i}{3}}=\cos\frac{2\pi}{3}+i\,\sin\frac{2\pi}{3}=-\frac{1}{2}+i\,\frac{\sqrt{3}}{2}$. So a splitting field of x^3-2 over $\mathbb{Q}$ is $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}\,\zeta, \sqrt[3]{2}\,\zeta^2]$ which is the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$, $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, and $\sqrt[3]{2}\zeta^2$. Then $\zeta=\sqrt[3]{2}\,\zeta/\sqrt[3]{2}$ is in this field; and so

Lecture 25: Existence of a splitting field

Monday, June 4, 2018 2:50 PM

$\zeta \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2]$. Hence $\mathbb{Q}[\sqrt[3]{2}, \zeta] \subseteq \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2]$.

Clearly $\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2 \in \mathbb{Q}[\sqrt[3]{2}, \zeta]$. So $\mathbb{Q}[\sqrt[3]{2}, \zeta]$ is a splitting field of x^3-2 over $\mathbb{Q}$.

Theorem. Suppose F is a field and $f(x) \in F[x]$ has positive degree. Then $f(x)$ has a splitting field over F.

Pf. We proceed by induction on $\deg(f)$.

Base. If $\deg(f) = 1$, then $f(x) = a_1 x + a_0$ and $a_1 \in F \setminus \mho$. Hence $f(x) = a_1 \left(x + \frac{a_0}{a_1}\right)$, $\frac{a_0}{a_1} \in F$; and so F is a splitting field of $f(x)$ over F.

Induction Step. $F[x]$ is a UFD. So $f(x) = \prod_{i=1}^{m} p_i(x)$ where $p_i(x)$ is irreducible in $F[x]$. Hence $\exists\ F \xhookrightarrow[\overline{i}]{} \overline{F}$ and $\alpha \in \overline{F}$ s.t. $\overline{i}(p_1)(\alpha) = 0$, (Hence $\overline{i}(f)(\alpha) = 0$) and $\overline{F}$ is the smallest ring that contains α and $i(F)$. Therefore by the factor theorem, $\exists\ \overline{f}(x) \in \overline{F}[x]$ s.t. $\deg \overline{f} = \deg f - 1$ and $f(x) = (x-\alpha)\overline{f}(x)$. Now by the induction hypothesis,

Lecture 25: Existence of a splitting field

Monday, June 4, 2018 11:29 AM

$\overline{f}$ has a splitting field over $\overline{F}$; that means

- $\exists$ a field E and $\hat{i}: \overline{F} \hookrightarrow E$ injective ring hom.
- $\exists\, \alpha_1, \ldots, \alpha_{n-1} \in E$, $\hat{i}(\overline{f})(x) = c(x-\alpha_1)\cdots(x-\alpha_{n-1})$ for some $c \in \overline{F}\setminus\{0\}$
- The smallest subfield of E that contains $\hat{i}(F)$ and $\alpha_1, \ldots, \alpha_{n-1}$ is E.

We go over this part of argument in the next lecture.

Consider.

$$\begin{tikzcd} F \arrow[r, hook, "\bar{i}"] \arrow[rr, hook, bend right, "i"'] & \overline{F} \arrow[r, hook, "\hat{i}"] & E \end{tikzcd}$$

- $$i(f)(x) = \hat{i}(\bar{i}(f)(x))$$
$$= \hat{i}((x-\alpha)\overline{f}(x))$$
$$= (x-\hat{i}(\alpha))\,\hat{i}(\overline{f})(x)$$
$$= c(x-\underbrace{\hat{i}(\alpha)}_{\alpha_n})(x-\alpha_1)\cdots(x-\alpha_{n-1}).$$

- A subfield of E that contains $i(F)$ and $\alpha_1, \ldots, \alpha_n$ contains $\hat{i}(\bar{i}(F))$ and $\hat{i}(\alpha)$; And so it contains $\hat{i}(\underbrace{\bar{i}(F)[\alpha]}_{\overline{F}})$ and $\alpha_1, \ldots, \alpha_{n-1}$.

Hence it should be E. ; and claim follows. ■