Content:

Example	What do elements in $\mathbb{Q}(\sqrt[3]{2})$ look like?
Example	What do elements in $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ look like?
Example	Splitting field of $x^3 - 2 = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}})$.
Example	Splitting field of $x^2 + 1 = \mathbb{Q}(i, -i) = \mathbb{Q}(i)$.
Theorem	If p is prime and n a positive integer, then there is a field with p^n elements.
Example	Construct a field of order 8.
Definition	An element $\alpha \in F$ is called a primitive element if α is a generator of F^*.
Corollary	For every prime p and positive integer n, there is an irreducible polynomial over $\mathbb{Z}_p$ of degree n.

Announcements April 5, Monday, Field Extension, Part II, #2, 5.

Recap

$p(x) \in F[x]$.

$\varphi: F' \to F$ defined by $r + I \mapsto r$.

$\varphi^*: F'[x] \to F[x]$ is defined by

$c_0 + I + (c_1 + I)x + \cdots \mapsto c_0 + c_1x + \cdots + c_nx^n$.

$p(x) \in F[x]$ is the isomorphic image of $\overline{p}(x) \in F'[x]$

We showed $d = x + I$ is a root of $\overline{p}(x)$.

$E = F[x]/I$ where $I = (p(x))$

$\cup|$

$F' = \{a + I | a \in F\} \cong F$.

Example What do elements in $\mathbb{Q}(\sqrt[3]{2})$ look like? $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}$

Proof: $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$.

Example What do elements in $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ look like? $a_0 + a_1\sqrt[3]{2}e^{\frac{2\pi i}{3}} + a_2\sqrt[3]{2}e^{\frac{2\pi i}{3}}$

Proof: $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}}) \cong \mathbb{Q}[x](x^3 - 2)$.

And $\sqrt[3]{2}e^{\frac{4\pi i}{3}}$ is a third root of $x^3 - 2$.

$\mathbb{Q} \cong \mathbb{Q}' = \{r + I\}\ r \in \mathbb{Q}\} \subseteq \mathbb{Q}[x]/(x^3 - 2) = E$.

$p(x) = x^3 - 2$. $\overline{p}(x) = (1 + I)x^3 - (2 + I) \in \mathbb{Q}'[x]$.

$\alpha = x + I$ is a root of $\overline{p}(x)$.

$\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$.

Recall $\varphi_{\sqrt[3]{2}}: \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}(\sqrt[3]{2})$ defined by $\varphi_{\sqrt[3]{2}}(x + I) = \sqrt[3]{2}$ or

$\varphi_{\sqrt[3]{2}e^{\frac{2\pi i}{3}}}: \mathbb{Q}[x]/(x^3 - 2) \cong \mathrm{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ defined by $\varphi_{\sqrt[3]{2}e^{\frac{2\pi i}{3}}}(x + I) = \sqrt[3]{2}e^{\frac{2\pi i}{3}}$.

$p(x) = x^3 - 2$. Do all the roots of $p(x)$ appear in $\mathbb{Q}(\sqrt[3]{2})$? No.

$p(\mathrm{x}) = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$

or $= (x - \sqrt[3]{2}e^{\frac{2\pi i}{3}})(x^2 + \sqrt[3]{2}e^{\frac{2\pi i}{3}}x + \sqrt[3]{4}e^{\frac{2\pi i}{3}})$

or $= (x - \sqrt[3]{2}e^{\frac{4\pi i}{3}})(x^2 + \sqrt[3]{2}e^{\frac{4\pi i}{3}}x + \sqrt[3]{4}e^{\frac{4\pi i}{3}})$

Example Splitting field of $x^3 - 2 = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}})$.

Example Splitting field of $x^2 + 1 = \mathbb{Q}(i, -i) = \mathbb{Q}(i)$. This is nice, but won't always happen.

Theorem If p is prime and n a positive integer, then there is a field with p^n elements.

Proof:
We know there are fields of order 2. $\mathbb{Z}_2$ is a field.
Assume $p^n > 2$. Let $g(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$.
By Kronecker, there is an extension k such that $g(x)$ splits over k.
So, k is an extension of $\mathbb{Z}_p$, hence char $(k) = p$, by HW6, #6.
Let $E = \{\alpha \in k \mid g(\alpha) = 0\}$. Claim: E is a field of order p^n.

We first show $|E| = p^n$.
Since deg $g = p^n$, $|E| \le p^n$. $g'(x) = p^n x^{p^n - 1} - 1 = -1$ (since char $(k) = p$).
Thus $g(x)$ and $g'(x)$ are relatively prime, hence $g(x)$ has no repeated roots, by HW7, #1(d)). Thus $|E| = p^n$.

We next show E is a commutative ring with unity.
$g(1) = 0$, so $1 \in E$. $E \subseteq k$ so multiplication is commutative.
Let $a, b \in E$. Note that since $g(a) = 0$, then $a^{p^n} - a = 0$ and $b^{p^n} - b = 0$.
So $g(ab) = (ab)^{p^n} - ab = a^{p^n}b^{p^n} - ab = ab - ab = 0$. Thus, $ab \in E$. And
$g(a - b) = (a - b)^{p^n} - (a - b) = a^{p^n} - b^{p^n} - (a - b) = (a - b) - (a - b) = 0$.
Thus $a - b \in E$. And hence E is a subring of k.
Let $a \in E$, $a \neq 0$. Note that E is a subring of a field k implies that E is an integral domain. Since $a^{p^n} = a$ then by cancellation we have $a^{p^n - 1} = 1$.
Since $p^n > 2$, then $p^n - 2 > 0$. And closure under multiplication in E gives us that $a^{p^n - 2} \in E$. So then $1 = a^{p^n - 1} = a(a^{p^n - 2}) \Rightarrow a^{p^n - 2} = a^{-1} \in E$.
Thus E is a field with p^n elements.

Note We don't really use this theorem to construct the fields.

Example Construct a field of order 8.
Let $g(x) = x^8 - x \in \mathbb{Z}_2[x]$. By Kronecker's Thm., there is a field k such that $g(x)$ splits over k. Let $E = \{a \in k \mid g(a) = 0\}$.
Then $E = \{0, 1, a_1, a_2, a_3, a_4, a_5, a_6\}$.
But we don't know much about the structure of E.

Definition An element $\alpha \in F$ is called a *primitive element* if α is a generator of F^*.

Corollary For every prime p and positive integer n, there is an irreducible polynomial over $\mathbb{Z}_p$ of degree n.

Proof:
Let E be an extension of $\mathbb{Z}_p$ such that $|E| = p^n$. By the preceding theorem, we know E exists.
By Theorem 3.30 (If k is a field and G is a finite subgroup of the multiplicative group $k^\cdot$, then G is cyclic. In particular, if k itself is finite (e.g. $k = \mathbb{Z}_p$), then $k^\cdot$ is cyclic.) we know that $E^* = E - \{0\}$ is a cyclic group.
Let $\alpha \in E$ be a primitive element.
Claim: $E = \mathbb{Z}_p(\alpha)$.
$\mathbb{Z}_p \subseteq E$ and $\alpha \in E$, so $\mathbb{Z}_p(\alpha) \subseteq E$.
Let $c \in E^*$. Then $c = \alpha^k$ for some k since α generates E^*.
Since $\alpha^k \in E^*$ then $E^* \subseteq \mathbb{Z}_p(\alpha)$.
Also $0 \in \mathbb{Z}_p(\alpha)$. Thus $E \subseteq \mathbb{Z}_p(\alpha)$. And now we have $E = \mathbb{Z}_p(\alpha)$.

Since $|E| = p^n$ and E is an extension of $\mathbb{Z}_p$, then $[E:\mathbb{Z}_p] = n$.
(Vector Space HW #9 gives us that $[E:\mathbb{Z}_p] = n \Rightarrow |E| = p^n$. The converse is easily proven to be true also.)
So $\mathbb{Z}_p(\alpha)/\mathbb{Z}_p$ is a finite extension.
Hence α is algebraic over $\mathbb{Z}_p$, by Theorem 38, Ext. Fields, Part I (If [E:F] $< \infty$, then E is algebraic over F.)
So there exists $f(x) \in \mathbb{Z}_p[x]$ such that $f(x)$ is irreducible and α is a root.
Hence there is $g(x)$, an irreducible factor of $f(x)$ such that α is a root.
By Theorem LN 3/10/10 (If E/F is an extension, $a \in E$, and a is algebraic over F, then $F(a) \cong F[x](p(x))$ where $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root.)we have $\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(g(x))$,
Moreover $n = [\mathbb{Z}_p(\alpha):\mathbb{Z}_p] = \deg g(x)$, by Lecture Notes 3/10/10 (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, deg $p(x) = n$, then … $[F(a):F] = n$.)
Thus we have an irreducible polynomial over $\mathbb{Z}_p$ of degree n.