- Find the $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$

Solution

$\mathbb{Q}(\sqrt{2})$ is a degree 2 extension of $\mathbb{Q}$

Since $\sqrt{2}$ has min. poly x^2-2 over $\mathbb{Q}$

$\therefore$ $\mathbb{Q}(\sqrt{2})$ is a dim 2 v. space over $\mathbb{Q}$ with basis $\{1, \sqrt{2}\}$

$\mathbb{Q}(\sqrt{3})$ is a 2. dim v. space over $\mathbb{Q}$, basis $\{1, \sqrt{3}\}$

$\mathbb{Q}(i)$ is a 2 dim v. space over $\mathbb{Q}$, with basis $\{1, i\}$

min poly is x^2-3

$$[\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$
$$= 2 \cdot 2 = 4$$

Then $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

min poly is x^2+1

$$[\mathbb{Q}(i, \sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})]\,[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$$
$$= 2 \cdot 4 = 8$$

with basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$ being

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}, i, i\sqrt{2}, i\sqrt{3}, i\sqrt{6}\}$$

Ex)

Let E, F be subfields of $GF(p^n)$,

$|E| = p^r$, $|F| = p^s$

Find $|E \cap F|$

Solution: I we know $E \cong GF(p^r)$, $F \cong GF(p^s)$

If $t \mid r$ and $t \mid s$ we know (from Thm)

there exists a unique isomorphic copy of $GF(p^t)$
in E an F, and aslo in $GF(p^n)$ (Since $r \mid n$, $s \mid n$) ← From same thm

$\Rightarrow \exists$ a uniqe copy of $GF(p^t)$ in $E \cap F$
for all $t \mid r$, $t \mid s$.

Since all finite fields are isomorphiz to $GF(p^j)$,

then $E \cap F \cong GF(p^j)$ for some j

Since if $\alpha \in E \cap F$, $\alpha \in GF(p^t) \Rightarrow GF(p^t)$
(upto iso) is in $E \cap F$

$\therefore$ $E \cap F$ must contain all $GF(p^t)$ s.t $t \mid r$ and $t \mid s$

$\Rightarrow E \cap F \cong GF(p^{\gcd(r,s)})$

$\therefore$ $|E \cap F| = p^{\gcd(r,s)}$
and $E \cap F$ is (isomorphiz to) a degree $\gcd(r,s)$
field ext. of $\mathbb{Z}_p$. ∎

$$\mathbb{Z}_2[x]/\langle x^3+x+1\rangle \cong \mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$$

proof

Method 1

$p(x)$, $q(x)$ are irreducible

$\therefore$ they are the min poly. of at least one of thier, say α_p, α_q are the roots

From thm.

$$\mathbb{Z}_2(\alpha_p) \cong \mathbb{Z}_2[x]/\langle p(x)\rangle$$

$$\mathbb{Z}_2(\alpha_q) \cong \mathbb{Z}_2[x]/\langle q(x)\rangle$$

and these are simple ext. of $\mathbb{Z}_2$ of degree 3

$\therefore$ By thm $\mathbb{Z}_2(\alpha_p) = \text{Span}_{\mathbb{Z}_2}\{1, \alpha_p, \alpha_p^2\}$

$$\mathbb{Z}_2(\alpha_q) = \text{Span}_{\mathbb{Z}_2}\{1, \alpha_q, \alpha_q^2\}$$

$\therefore$ $|\mathbb{Z}_2(\alpha_p)| = |\mathbb{Z}_2(\alpha_q)| = 2^3$

$\therefore$

$$\mathbb{Z}_2(\alpha_p) \cong \mathbb{Z}_2(\alpha_q) \cong GF(2^3).$$

Method 2

Since $p(x), q(x)$ are irr. then

$\mathbb{Z}_2[x]/\langle p(x)\rangle$, $\mathbb{Z}_2[x]/\langle q(x)\rangle$ are fields

Fact:
By the division alg. we know that every $f(x) \in F[x]$ has a unique (up to constant mult.) representive in

$F[x]/\langle p(x)\rangle$ namely

$f(x) = q(x)\,p(x) + r(x)$, $\deg(r) < \deg(p)$

So $f(x) = r(x) \in F[x]/\langle p(x)\rangle$

By above, we have that any $g(x) \in F[x]$ with degree <u>less</u> than $p(x)$ must represent itself and that these are all unique (Eq. classes) in the Quotient.

$\therefore E = \mathbb{Z}_2[x]/\langle p(x)\rangle = \{ r(x) + \langle p(x)\rangle \mid \deg(r(x)) \leq 2 \}$

↑ there are 8 unique poly. Of degree ≤ 2 in $\mathbb{Z}_2[x]$

$\alpha = x + \langle p(x)\rangle$ is always a root of $p(x)$ in E

$\mathbb{Z}_2(\alpha) \cong \mathbb{Z}_2[x]/\langle p(x)\rangle$ (if α is alg. and $p(x)$ is min. poly of α)