Solutions to Asst. 11 - MA542

Chapter 21:

4) Recall that E is alg. closed iff every polynomial $f(x) \in E[x]$ splits in $E[x]$.

Suppose E is not alg closed. Then $\exists E'/E$, $\alpha \in E'$, $\alpha \notin E$, α alg over E. Then α is alg over F. Let $f(x)$ be the min poly of α over F & $g(x)$ its min poly over E. If $f(x)$ splits in E, then, since $g(x) \mid f(x)$ in $E[x]$ & $g(x)$ is irred in $E[x]$, $\Rightarrow g(x)$ is a degree one polynomial. But this implies that $\alpha \in E$. Contradiction, hence $f(x)$ doesn't split in E. QED

Chapter 22:

2) $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] = n$ so $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$ QED

12) Since $\mathbb{F}_{2^5}$ is a subfield of $\mathbb{F}_{p^n}$ iff $p=2$ & $5 \mid n$, this implies that we are looking at fields $\mathbb{F}_{2^n}$ w/ $n = 5m$ & $m \geq 1$.

$\mathbb{F}_{2^5}$ needs to be a proper subfield so $m \geq 2$. But also the largest proper subfield, so $m \leq 5$ (since, if $m > 5$, $n = 5m$ has a factor > 5, namely m, so $\mathbb{F}_{2^m}$ is a larger proper subfield)

So the finite fields with $\mathbb{F}_{2^5}$ as largest proper subfield are $\boxed{\mathbb{F}_{2^{10}}, \mathbb{F}_{2^{15}}, \mathbb{F}_{2^{20}}}$ ($10 \mid 20$ so $\mathbb{F}_{2^{10}} \subseteq \mathbb{F}_{2^{20}}$)

14) The set of subfields of $\mathbb{F}_{p^n}$ only depends on n (it is independent of p), so the smallest field with exactly 6 subfields will have $p=2$.

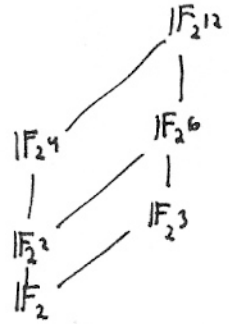
subfields of $\mathbb{F}_{p^n}$ = # divisors of n.

if n is prime it has two divisors: $\{1, n\}$ so we don't need to consider them

n (composite number)	divisors
4	1, 2, 4
6	1, 2, 3, 6
8	1, 2, 4, 8
9	1, 3, 9
10	1, 2, 5, 10
12	1, 2, 3, 4, 6, 12

6 divisors

So $\mathbb{F}_{2^{12}}$ is the smallest field with exactly 6 subfields



28) Let $p(x) \in \mathbb{F}_p[x]$ with no multiple zeroes. Let E be its splitting field over $\mathbb{F}_p$. Then $E/\mathbb{F}_p$ is a finite extension so E is a finite field containing $\mathbb{F}_p$, so $\exists n \geq 1$ s.t. $E = \mathbb{F}_{p^n}$. Then every element of E is a root of $f(x) = x^{p^n} - x$. Hence, every root of $p(x)$ is a root of $f(x)$ so $p(x) \mid f(x)$ (since $p(x)$ has distinct roots. Formally: $(x-\alpha_i) \mid p(x) \Rightarrow (x-\alpha_i) \mid f(x)$ & $p(x) = \prod_{i=1}^{m} (x-\alpha_i)$ with α_i distinct.)

3) Let F be a finite field. Then $\exists p, n$ s.t. $F = \mathbb{F}_{p^n}$. Then $E = \mathbb{F}_{p^{2n}}$ is an ext'n of F with $E \supsetneq F$ & E/F alg. hence F is not alg closed.

Questions:

1)
$$\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array}$$

so $[L:F] = [L:K][K:F]$ so $[L:F] = [L:K] \Rightarrow [K:F] = 1$. So $\dim_F K = 1$.

Then $\exists \alpha \in K$ s.t. $\forall \beta \in K$, $\exists! a_\beta \in F$ s.t. $\beta = \alpha a_\beta$

& taking $\beta = 1 \in K$, $\exists! \gamma \in K$ s.t. $\alpha\gamma = 1$ namely $\gamma = \alpha^{-1}$. So $a_1 = \alpha^{-1}$

$\Rightarrow \alpha^{-1} \in F \Rightarrow \alpha \in F$ so $\forall \beta \in K$ $\beta = \alpha a_\beta$ with $\alpha \& a_\beta \in F$ so $\beta \in F$ so $K = F$

QED

2) Let $a = \sqrt{3}$, $b = 2^{1/4}$. The min poly of a over $\mathbb{Q}$ is $p(x) = x^2 - 3$

. . . . . b . . . . . $q(x) = x^4 - 2$

so the roots of $p(x)$ are $a_1 = a = \sqrt{3}$, $a_2 = -\sqrt{3}$

. . . . . $q(x)$ . . . . $b_1 = b = 2^{1/4}$, $b_2 = i2^{1/4}$, $b_3 = -2^{1/4}$, $b_4 = -i2^{1/4}$ (i.e. for $1 \le j \le 4$, $b_j = i^{j-1}2^{1/4}$)

look at values of $e_{jk} := \frac{a_k - a}{b - b_j}$ for $1 \le k \le 2$, $2 \le j \le 4$. The numerator is either 0 or $-2\sqrt{3}$

The denominator is one of $b_1 - b_2 = 2^{1/4}(1-i)$, $b_1 - b_3 = 2 \cdot 2^{1/4}$, $b_1 - b_4 = 2^{1/4}(1+i)$

so $e_{jk} \in \left\{0, \frac{2^{3/4}\sqrt{3}}{(i-1)}, \frac{-\sqrt{3}}{2^{1/4}}, \frac{-2^{3/4}\sqrt{3}}{1+i}\right\}$ so $e_{jk} \neq 1$ $\forall j,k$

let $d = 1$, let $\boxed{c = a + db = \sqrt{3} + 2^{1/4}}$, Then $\boxed{\mathbb{Q}(a,b) = \mathbb{Q}(c)}$ QED