Solutions to Assignment 8 – MA542

Chapter 20:

2) $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$: take $\sqrt{2},\sqrt{3} \in \mathbb{C}$; since $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ ("closure under addition")

also, clearly, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$

but $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$, $\sqrt{2}$, & $\sqrt{3}$ (by defn)

so $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$

$\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$: as above, we just need to show that both $\sqrt{2}$ & $\sqrt{3}$ are in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ (it's clear that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$)

$a_1 := (\sqrt{2}+\sqrt{3})^2 = 2+3+2\sqrt{2}\sqrt{3} \in F := \mathbb{Q}(\sqrt{2}+\sqrt{3})$

& clearly, $2,3 \in F$ so $a_2 := \sqrt{2}\sqrt{3} = \frac{a_1-2-3}{2} \in F$

Then $a_1 a_2 \in F$ (since $a_1 a_2 = 2\sqrt{3}+3\sqrt{2}$) and $a_3 := \sqrt{2}+\sqrt{3} \in F$ by definition

so $a_1 a_2 - 2a_3 \in F$ (since $a_1 a_2 - 2a_3 = \sqrt{2}$)

so $\sqrt{2} \in F$

Then $(\sqrt{2}+\sqrt{3}) - \sqrt{2} \in F$ (since $(\sqrt{2}+\sqrt{3}) - \sqrt{2} = \sqrt{3}$)

QED

#7 on next page

8) $f(x) = x^3+x+1$ is irred. in $F[x]$ since it has no roots (& $\deg f \le 3$). Let $I = (f(x)) \subseteq F[x]$

Hence, $E := F[x]/(f(x)) = \{0\} \cup \{g(x)+I : \deg g \le \deg f = 3\}$

and each element of E is uniquely given in this way

ie. There's a bijection between E & $P_2(\mathbb{Z}/2\mathbb{Z})$ the 3-dim'l vector space over $\mathbb{Z}/2\mathbb{Z}$ of polynomials in $(\mathbb{Z}/2\mathbb{Z})[x]$ of deg ≤ 2.

Thus $\#E = 2^3 = 8$

Let $a \in F(a) \subseteq E$ be a root of $f(x)$. So $a^3+a+1=0$. Then $E = \{0, 1, a, a+1, a^2, a^2+1, a^2+a, a^2+a+1\}$

·	0	1	a	$a+1$	a^2	a^2+1	a^2+a	a^2+a+1
0	0	0	0	0	0	0	0	0
1	0	1	a	$a+1$	a^2	a^2+1	a^2+a	a^2+a+1
a	0	a	a^2	a^2+a	$a+1$	1	a^2+a+1	a^2+1
$a+1$	0	$a+1$	a^2+a	a^2+1	a^2+a+1	a^2	1	a
a^2	0	a^2	$a+1$	a^2+a+1	a^2+a	a	a^2+1	1
a^2+1	0	a^2+1	1	a^2	a	a^2+a+1	$a+1$	a^2+a
a^2+a	0	a^2+a	a^2+a+1	1	a^2+1	$a+1$	a	a^2
a^2+a+1	0	a^2+a+1	a^2+1	a	1	a^2+a	a^2	$a+1$

$a \cdot a^2 = a^3 = a+1$

$(a+1)^2 = a^2+1$

$(a^2)^2 = a^4 = a\,a^3 = a(a+1) = a^2+a$

$(a^2+1)^2 = a^4+1 = a^2+a+1$

$(a^2+a)^2 = a^4+a^2 = a^2+a+a^2 = a$

$(a^2+a+1)^2 = a^4+a^2+1 = a^2+a+a^2+1 = a+1$

$a^2(a+1) = a^3+a^2 = a+1+a^2$

$a(a^2+1) = a^3+a = a+1+a = 1$

$a(a^2+a) = a^3+a^2 = a^2+a+1$

etc

7) look for an irreducible polynomial $p(x) \in \mathbb{Q}[x]$, s.t. $p(\sqrt{1+\sqrt{5}}) = 0$

consider $p_1(x) = x^2 - (1+\sqrt{5}) \in \mathbb{Q}(\sqrt{5})[x]$. $a := \sqrt{1+\sqrt{5}}$ is a root of $p_1(x)$

(The other root is $-a$.) since $(1+\sqrt{5})(1-\sqrt{5}) = -4 \in \mathbb{Q}$ & $(1+\sqrt{5})+(1-\sqrt{5}) = 2 \in \mathbb{Q}$

can take $p(x) = (x^2 - (1+\sqrt{5}))(x^2 - (1-\sqrt{5})) = x^4 - (1+\sqrt{5})x^2 - (1-\sqrt{5})x^2 + (1+\sqrt{5})(1-\sqrt{5})$

$= x^4 - 2x^2 - 4$.

so a is a root of $p(x)$, & $p(x)$ is irred. so $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(a)$ QED

Alternatively, consider $a^2 = 1+\sqrt{5}$ & $a^4 = 1 + 2\sqrt{5} + 5$

Then $a^4 - 2a^2 = 6 + 2\sqrt{5} - 2(1+\sqrt{5}) = 4$

so a satisfies $p(x) = x^4 - 2x^2 - 4 = 0$ & $p(x) \in \mathbb{Q}$ QED

10) let $f(x) = x^3 + x + 1$; $f(a^2) = a^6 + a^2 + 1 = (a^3)^2 + a^2 + 1$

$= a^2 + 1 + a^2 + 1 = 0$

or $a^3 = a + 1$

$f(a^2+a) = (a^2+a)^3 + a^2 + a + 1$ "0"

$= a^6 + 3a^5 + 3a^4 + a^3 + a^2 + a + 1$

$= a^2(a^4 + a^3 + a^2 + 1)$

$= a^2((a^2+a) + (a+1) + a^2 + 1) = 0$ QED

16) $\beta \in E$ s.t. $\beta^4 = \beta + 1$. $f(x) = x^4 + x + 1$. What are the other roots of $f(x)$

an element $\alpha \in E$ is $\alpha = a_3\beta^3 + a_2\beta^2 + a_1\beta + a_0$, $a_i \in \mathbb{Z}/2\mathbb{Z}$

$\alpha^4 = (a_3\beta^3)^4 + (a_2\beta^2)^4 + (a_1\beta)^4 + a_0^4$

$= a_3(\beta+1)^3 + a_2(\beta+1)^2 + a_1(\beta+1) + a_0$

$= a_3(\beta^3 + \beta^2 + \beta + 1) + a_2(\beta^2 + 1) + a_1(\beta+1) + a_0$

$= a_3\beta^3 + (a_3 + a_2)\beta^2 + (a_3 + a_1)\beta + a_3 + a_2 + a_1 + a_0$

set equal to $\alpha + 1 = a_3\beta^3 + a_2\beta^2 + a_1\beta + (a_0 + 1)$

so: β^3 coeff $\Rightarrow a_3 = 0$. constant coeff $\Rightarrow a_2 + a_1 = 1$ so $a_2 = 1$ & $a_1 = 0$ or $a_2 = 0$ & $a_1 = 1$

and a_0 is arbitrary. So the 4 roots are: β, $\beta+1$, β^2, & β^2+1

so, in E, $f(x) = (x-\beta)(x-(\beta+1))(x-\beta^2)(x-(\beta^2+1))$ QED

Questions: (1) let $a \in R$ a zero divisor, let $b \neq 0$ s.t. $ba = 0$. let $f(x) = ax + 1$

If $f(x)$ has a root $\alpha \in R \supset R$, then $0 = b(a\alpha + 1) = ba\alpha + b = b$. contradiction ($b \neq 0$)