# Solutions to Assignment 9 - MA542

## Chapter 20:

30) $f'(x) = 4x^3 + 1 = 1$. So $f'(x)$ has no factors of deg $\geq 1$, so $f(x)$ & $f'(x)$ have no such common factors, so $f(x)$ has no multiple roots in any ext'n of $\mathbb{Z}/2\mathbb{Z}$. QED

32) $f'(x) = 21x^{20} + 18x^8 = 0$. So $f(x)$ itself is a common deg $\geq 1$ factor of $f(x)$ & $f'(x)$. Hence, $f(x)$ has multiple roots in some ext'n of $\mathbb{Z}/3\mathbb{Z}$. QED

34) Note that $g(x) = x^2+x+2$ & $h(x) = x^2+2x+2$ are both irreducible over $\mathbb{Z}/3\mathbb{Z}$ (since they have no roots & are of deg $\leq 3$)

To form the splitting field of $f(x) = g(x)h(x)$, take an irred. factor $p(x)$ of $f(x)$

Say $p(x) = g(x)$, then let $E = (\mathbb{Z}/3\mathbb{Z})[x]/(g(x))$. Define $\alpha := x + I$, $I := (g(x))$.

Then $\alpha$ is a root of $f(x)$ in $E$, so $\alpha^2 + \alpha + 2 = 0$.

The elements of $E$ are $\{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$ (because every non-zero element of $E$ is represented uniquely by a polynomial in $(\mathbb{Z}/3\mathbb{Z})[x]$ of deg $< \deg g(x) = 2$)

Think about whether any of these elements are roots of $g(x)$ or $h(x)$

Note: $\cdot\ h(2\alpha) = (2\alpha)^2 + 2\cdot 2\alpha + 2 = 2^2\alpha^2 + 2^2\alpha + 2 = \alpha^2 + \alpha + 2 = 0$ (↳ $4 = 1$ in $\mathbb{Z}/3\mathbb{Z}$)

so $2\alpha$ is a root of $h(x)$ in $E$.

$\cdot\ h(\alpha+1) = (\alpha+1)^2 + 2(\alpha+1) + 2 = \alpha^2 + 2\alpha + 1 + 2\alpha + 2 + 2 = \alpha^2 + \alpha + 2 = 0$

so $\alpha+1$ is a root of $h(x)$ in $E$

$\cdot\ g(2\alpha+2) = (2\alpha+2)^2 + (2\alpha+2) + 2 = 4\alpha^2 + 8\alpha + 4 + 2\alpha + 2 + 2 = \alpha^2 + \alpha + 2 = 0$

so $E$ contains 4 roots of $f(x)$: $\alpha, \alpha+1, 2\alpha, 2\alpha+2$

so the splitting field of $f(x)$ over $\mathbb{Z}/3\mathbb{Z}$ is $(\mathbb{Z}/3\mathbb{Z})(\alpha, \alpha+1, 2\alpha, 2\alpha+2)$. This is clearly $E$.

So over $E$, $\boxed{f(x) = (x-\alpha)(x-(\alpha+1))(x-2\alpha)(x-(2\alpha+2))}$

35) (i) by assumption $f(x)$ splits in $L$. (so we need to show $L$ is the smallest ext'n of $K$ in which $f(x)$ splits)

(ii) Let $E/K$ w/ $E \subsetneq L$ s.t. $f(x)$ splits in $E$. Then, $E/F$ & $f(x)$ splits in $E$, contradicting the fact that $L$ is the splitting field of $f(x)$ over $F$. QED

## Questions

(1) Note that $f(x) = x^3 - (\pi^3)^2 \in \mathbb{Q}(\pi^3)$ & $f(\pi^2) = (\pi^2)^3 - (\pi^3)^2 = 0$

let $g(x) = f(x+1) = (x+1)^3 - (\pi^3)^2 = x^3 + 3x^2 + 3x + 1 - \pi^6 \in \mathbb{Q}(\pi^3)$.

Then $g(\pi^2 - 1) = f(\pi^2) = 0$. So $\pi^2 - 1$ is alg. over $\mathbb{Q}(\pi^3)$ QED

(2) Rewrite the proof of Eisenstein Criterion in this analogous situation:

Lemma: $T$ is a prime in $D = (\mathbb{Z}/p\mathbb{Z})[T]$

proof: $D/(T) \cong \mathbb{Z}/p\mathbb{Z}$ so $(T)$ is maximal, hence prime, so $T$ is prime (since prime elements are exactly the ones whose associated principal ideals are prime). QED

Now, suppose $f(x) = g(x)h(x)$ with $g(x)h(x) \in F[x]$, $1 \le \deg g(x)$ & $1 \le \deg h(x) < n$

write $g(x) = \sum_{i=0}^{r} b_i x^i$, $b_i \in D$, $h(x) = \sum_{i=0}^{s} c_i x^i$, $c_i \in D$ (by Gauss' lemma)

Since $T \mid a_0 = b_0 c_0$, but $T^2 \nmid a_0 = b_0 c_0$ (& $T$ is prime), this means $T$ only divides one of $b_0$ and $c_0$. wlog $T \mid b_0$, $T \nmid c_0$. Since $T \nmid a_n = b_r c_s$, so $T \nmid b_r$ & $T \nmid c_s$.

Let $k$ be the least integer s.t. $T \nmid b_k$. Consider $a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$.

by assumption, $T \mid a_k$ & $T \mid b_i$ for $i < k$. so $T \mid a_k - (b_{k-1} c_1 + \cdots + b_0 c_k) = b_k c_0$.

But $T \nmid b_k$ & $T \nmid c_0$. Since $T$ is prime, this implies a contradiction (namely $T \nmid b_k c_0$) QED

(3) Let $F = (\mathbb{Z}/p\mathbb{Z})(T)$. For $n \in \mathbb{Z}_{>1}$, let $f_n(x) = x^{p^n} - T$

Then $f_n'(x) = p^n x^{p^n - 1} = 0$ so $f_n(x)$ has multiple roots (since $f_n(x)$ is a common factor of $f_n(x)$ & $f_n'(x)$)

By the Eisenstein criterion of question (2), $f_n(x)$ is irred. & hence inseparable. QED