Homework #11 Solutions

p 348, #12 Since $\pi^3 \in F$, π is a root of the polynomial $x^3 - \pi^3 \in F[x]$. This polynomial is irreducible over F since the only possible root in F would be π itself, and it is easy to show that $\pi \notin F$ (if it were, π would be algebraic over $\mathbb{Q}$). Therefore a basis for $F(\pi)$ over F is $\{1, \pi, \pi^2\}$.

p 348, #14 Let $F = \mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2 \,|\, a, b, c \in \mathbb{Q}\}$ and $\phi : F \to F$ be an automorphism. Arguing as we have several times before, we can show that $\phi(r) = r$ for all $r \in \mathbb{Q}$. It follows that $5 = \phi(5) = \phi((\sqrt[3]{5})^3) = \phi(\sqrt[3]{5})^3$. Since $\phi(\sqrt[3]{5}) \in F \subset \mathbb{R}$, we can therefore conclude that $\phi(\sqrt[3]{5}) = \sqrt[3]{5}$. Finally, this means that

$$\begin{aligned} \phi(a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2) &= \phi(a) + \phi(b)\phi(\sqrt[3]{5}) + \phi(c)\phi(\sqrt[3]{5})^2 \\ &= a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2 \end{aligned}$$

for any rational a, b, c. But every element of F can be written in the form above, and so it must be that $\phi(\alpha) = \alpha$ for every $\alpha \in F$. That is, the only automorphism of F is the identity.

p 348, #20 Since $a, b, c \in F(c)$ and $F(c)$ is a field, $ac + b \in F(c)$. From this it follows that $F(ac + b) \subset F(c)$. Since $a, b, ac + b \in F(ac + b)$, $a \neq 0$ and $F(ac + b)$ is a field, $c = a^{-1}((ac + b) - b) \in F(ac + b)$. This gives $F(c) \subset F(ac + b)$. Having established the necessary containments, we conclude that $F(c) = F(ac + b)$.

p 348, #26 It is straightforward to verify that

$$x^8 - x = x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

over $\mathbb{Z}_2$. This is the desired factorization since both $x^3 + x + 1$ and $x^3 + x^2 + 1$ have no zeros in $\mathbb{Z}_2$ and are therefore irreducible over $\mathbb{Z}_2$.

p 367, #30 If $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ then $f'(x) = 1$. It follows that $f(x)$ and $f'(x)$ cannot have common positive degree factors and therefore that $f(x)$ does not have any multiple roots.

p 367, #32 If $f(x) = x^{21} + 2x^9 + 1 \in \mathbb{Z}_3[x]$ then $f'(x) = 0$ so that $f(x)$ is a common positive degree factor of both $f(x)$ and $f'(x)$. It follows that $f(x)$ must have multiple roots.

p 367, #34 Since $\mathbb{Z}_3$ has characteristic different from 2, we can apply the quadratic formula to conclude that the roots of x^2+x+2 are

$$\frac{-1 \pm \sqrt{-7}}{2} = 2(-1 \pm \sqrt{2}) = 1 \pm 2\sqrt{2} = 1 \pm \sqrt{2}$$

and the roots of x^2+2x+2 are

$$\frac{-2 \pm \sqrt{-4}}{2} = 2(-2 \pm \sqrt{2}) = 2 \pm 2\sqrt{2} = 2 \pm \sqrt{2}.$$

Therefore, the splitting field of the indicated polynomial is $\mathbb{Z}_3[\sqrt{2}]$. Since we have the 4 roots of our polynomial we know that it may be factored over this field as

$$(x-(1+\sqrt{2}))(x-(1-\sqrt{2}))(x-(2+\sqrt{2}))(x-(2-\sqrt{2})).$$

Handout, #1 If $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, then the fact that we are working in characteristic p implies that $f'(x) = -1$. Therefore $f(x)$ and $f'(x)$ cannot have positive degree factors in common and so $f(x)$ does not have multiple roots.

Handout, #2 Recall that $a^p = a$ for all $a \in \mathbb{Z}_p$. Therefore, if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$ then, since we are working in characteristic p

$$\begin{aligned}
(f(x))^p &= (a_n x^n)^p + (a_{n-1}x^{n-1})^p + \cdots + a_0^p \\
&= a_n^p x^{np} + a_{n-1}^p x^{(n-1)p} + \cdots + a_0^p \\
&= a_n (x^p)^n + a_{n-1}(x^p)^{n-1} + \cdots + a_0 \\
&= f(x^p).
\end{aligned}$$

Handout, #3 Let $g(x) = x^p - x + 1$. Let α be a root of $g(x)$ in some extension E of $\mathbb{Z}_p$. Notice first that $\alpha \notin \mathbb{Z}_p$, since otherwise we would have $\alpha^p = \alpha$ and $g(\alpha) = 1 \neq 0$. Now notice that since we are working in characteristic p, $\alpha + 1$ is also a root of $g(x)$:

$$g(\alpha+1) = (\alpha+1)^p - (\alpha+1) + 1 = \alpha^p + 1 - \alpha - 1 + 1 = g(\alpha) = 0.$$

Furthermore, since α was an arbitrary root of $g(x)$ we can apply this result to conclude that, in fact, $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1$ are all distinct roots of $g(x)$. Since $\deg g(x) = p$ these must indeed be all of the roots of $g(x)$.

Now assume that $g(x)$ is reducible over $\mathbb{Z}_p$. Then $g(x) = f(x)h(x)$ for some $f(x), g(x) \in \mathbb{Z}_p[x]$ with $1 \leq \deg f(x) \leq p-1$. It follows that the roots of $f(x)$ must be a nonempty proper subset of $\{\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1\}$. Hence, in $E[x]$ we may factor $f(x)$ as

$$f(x) = (x-(\alpha+i_1))(x-(\alpha+i_2))\cdots(x-(\alpha+i_n))$$

where each $i_j \in \mathbb{Z}_p$. The coefficient of x^{n-1} in the polynomial on the right is $-n\alpha - (i_1+i_2+\cdots i_n)$ and since $f(x) \in \mathbb{Z}_p[x]$, this coefficient must belong to $\mathbb{Z}_p$. Since $i_1+i_2+\cdots+i_n \in \mathbb{Z}_p$, it follows that $n\alpha \in \mathbb{Z}_p$. But $n = \deg f(x)$ and so $1 \leq n \leq p-1$, i.e. n is a unit in $\mathbb{Z}_p$. We conclude that $\alpha \in \mathbb{Z}_p$, which, according to our work in the preceding paragraph, is a contradiction. This means that $g(x)$ must actually be irreducible over $\mathbb{Z}_p$.