Homework 7 Solutions

Ch 19: 1 – 3, 14 – 16, 20, 22, 24, 25, 36, 37, 43, 44, 47

1. Describe $\mathbb{Q}(\sqrt[3]{5})$.

$\mathbb{Q}(\sqrt[3]{5}) = \mathbb{Q}[x]/\langle x^3 - 5\rangle$ so one description is as the set of all elements $q(x) + \langle x^3 - 5\rangle$, where $q(x) = a_0 + a_1 c + a_2 x^2$ (by Euclidean algorithm). Letting $\alpha = x + \langle x^3 - 5\rangle$, or if you like, let $\sqrt[3]{5} = x + \langle x^3 - 5\rangle$, then the elements of $\mathbb{Q}[x]/\langle x^3 - 5\rangle$ are of the form $a_0 + a_1\alpha + a_2\alpha^2$ so that

$$\mathbb{Q}(\sqrt[3]{5}) = \{a_0 + a_1(5^{1/3}) + a_2(5^{2/3}) \mid a_0, a_1, a_2 \in \mathbb{Q}\}$$

Another less useful description is $\mathbb{Q}(\sqrt[3]{5})$ is the smallest field containing $\mathbb{Q}$ as a subfield with a root of $x^3 - 5$.

2. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Clearly, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ so to get equality, we just need $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Notice, $(\sqrt{2} + \sqrt{3})(\sqrt{2} + \sqrt{3}) = 2 + 2\sqrt{6} + 3 \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. So $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. This means $(\sqrt{2} + \sqrt{6})(\sqrt{2} + \sqrt{6}) = 2 + 2\sqrt{2}\sqrt{6} + 6 = 8 + 4\sqrt{3}$, so $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Similarly, $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

3. Find the splitting field of $x^3 - 1$. Let $\omega = e^{i\frac{2\pi}{3}}$ be the principle cubic root unity. Then $x^3 - 1$ has roots $1, \omega, \omega^2$ and so $\mathbb{Q}(\omega)$ is the splitting field.

14. Find all ring automorphisms of $\mathbb{Q}(\sqrt{5})$ and of $\mathbb{Q}(\sqrt[3]{5})$.

The automorphisms must take roots of the irreducible polynomial to each other. So for $x^2 - 5$ the roots are $\pm\sqrt{5}$, and thus there are two automorphisms, the identity, and $\sqrt{5} \mapsto -\sqrt{5}$.

For $x^3 - 5$ the roots are $\sqrt[3]{5}\,\omega^m$ for $m = 0, 1, 2$ where $\omega = e^{i\frac{2\pi}{3}}$. Since any automorphism of $\mathbb{Q}(\sqrt[3]{5})$ must send $\sqrt[3]{5}$ to one of $\sqrt[3]{5}\,\omega^m$ for $m = 0, 1, 2$, there is only one possibility. Namely, $\sqrt[3]{5}$ must be fixed, and hence there is only the identity automorphism.

Note This is a different question, than understanding the automorphisms of the splitting field $\mathbb{Q}(\sqrt[3]{5}, \omega)$, i.e., $\mathrm{Gal}(x^3 - 5)$.

15. Let F be a field of characteristic p and let $f(x) = x^p - a$ show that f either splits or is irreducible over F.

Let α be a root of $f(x)$ in a field $F \subseteq E$ (possibly $E = F$), since E is also of characteristic p we have $\alpha^p - a = 0$ so $a = \alpha^p$ and $f(x) = x^p - \alpha^p = (x - \alpha)^p$. If $\alpha \in F$, then $f(x)$ splits over F.

If $\alpha \notin F$ let $g(x)$ be an irreducible factor of $f(x)$. We know, in E, that $g(x) = (x - \alpha)^k$ for some $1 < k < p$ since $f(x) = (x - \alpha)^p$, but then $g(x) = h(x^p)$ (Theorem 19.6) and so it must be that $k = p$, hence $f(x) = g(x)$, that is, $f(x)$ is irreducible.

16. Suppose β is a zero of $f(x) = x^4 + x + 1$ in some field extension E of $\mathbb{Z}_2$. Write $f(x)$ as a product of linear factors in $E[x]$.

We can perform polynomial division:

$$
\begin{array}{r|l}
 & x^3 + \beta x^2 + \beta^2 x + (1 + \beta^3) \\
\hline
x - \beta & x^4 + x + 1 \\
 & \underline{x^4 - \beta x^3} \\
 & \quad \beta x^3 \\
 & \quad \underline{\beta x^3 - \beta^2 x^2} \\
 & \qquad \beta^2 x^2 + x \\
 & \qquad \underline{\beta^2 x^2 - \beta^3 x} \\
 & \qquad\quad (1 + \beta^3)x + 1 \\
 & \qquad\quad \underline{(1 + \beta^3)x - \beta(1 + \beta^3)} \\
 & \qquad\qquad\qquad \beta^4 + \beta + 1 = 0
\end{array}
$$

Now

$$
\begin{aligned}
x^3 + \beta x^2 + \beta^2 x + \beta^3 + 1 &= x^2(\beta + x) + \beta^2(\beta + x) + 1 \\
&= (x^2 + \beta^2)(x + \beta) + 1 = (x + \beta)^2(x + \beta) + 1 \quad = (x + \beta)^3 + 1 \\
&= (x + \beta)^3 - 1 \\
&= (x + \beta - 1)((x + \beta)^2 + (x + \beta) + 1)
\end{aligned}
$$

Now

$$
\begin{aligned}
(x + \beta)^2 + (x + \beta) + 1 &= x^2 + \beta^2 + x + \beta + 1 \\
&= x^2 + \beta^2 + x + \beta^4 \qquad\qquad (\text{since } \beta^4 = -(1 + \beta) = 1 + \beta) \\
&= (x + \beta^2)(x + \beta^2 + 1)
\end{aligned}
$$

So

$$x^4 + x + 1 = (x - \beta)(x + \beta - 1)(x + \beta^2)(x + \beta^2 + 1)$$

20. Find $p(x)$ in $\mathbb{Q}[x]$ so that $\mathbb{Q}\left(\sqrt{1 + \sqrt{5}}\right) = \mathbb{Q}[x]/\langle p(x) \rangle$

$$
\begin{aligned}
x^2 &= 1 + \sqrt{5} \\
x^2 - 1 &= \sqrt{5} \\
(x^2 - 1)^2 &= 5 \\
x^4 - 2x^2 - 4 &= 0
\end{aligned}
$$

We cannot use Theorem 17.4 (Eisenstein's Criteria) to see that $p(x) = x^4 - 2x^2 - 4$ is irreducible. If $p(x)$ were reducible, then $x^4 - 2x^2 - 4 = (x^2 + ax + b)(x^2 + cx + d)$ with $a, b \in \mathbb{Z}$. Since $ax^3 + cx^3 = 0$ we have $c = -a$ and hence we have $x^4 - 2x^2 - 4 = (x^2 + ax + b)(x^2 - ax + d)$. Now we have $adx - abx = 0$, so either $a = 0$ or $b = d$. $b = d$ is not possible since $b^2 \neq -4$ and $a = 0$ is also not possible since then $x^4 - 2x^2 - 4 = (x^2 + b)(x^2 + d) = x^4 + (b + d)x + bd$ with $b + d = -2$ and $bd = -4$, hence $b = -2 - d$ and $(-2 - d)d = -2d + d^2 = -4$ or $d^2 - 2d + 4 = 0$ for an integer d. With some effort, we have shown that $p(x)$ is irreducible.

22. Suppose $f(x)$ and $g(x)$ are relatively prime in $F[x]$ and K is an extension field of F, then $f(x)$ and $g(x)$ remain relatively prime in $K[x]$.

If $f(x)$ and $g(x)$ are relatively prime in $F[x]$, this means that there are $h(x)$ and $k(x)$ in $F[x]$ so that $h(x)f(x)+k(x)g(x) = 1$. (Recall $f(x)$ and $g(x)$ are relatively prime if there is $l(x)$ a non-unit with $l(x) \mid f(x), g(x)$.) But since $F[x]$ is a PID, this means that $(f(x)) + (g(x)) = F[X]$ and this, in turn, means that the desired $h(x)$ and $k(x)$ exist.

But then, $h(x)f(x)+k(x)g(x) = 1$ continues to hold in $K[x]$ so $f(x)$ and $g(x)$ remain relatively prime.

24. Describe the elements of $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}(\sqrt{2})$.

$\mathbb{Q}[x]/\langle x^4 - 2\rangle = \mathbb{Q}(\sqrt{2})[x]/\langle x^2 - \sqrt{2}\rangle = \mathbb{Q}(\sqrt[4]{2})$ and so

$$\mathbb{Q}(\sqrt[4]{2}) = \left\{a + b\sqrt[4]{2} \;\middle|\; a, b \in \mathbb{Q}(\sqrt{2})\right\} = \left\{a + b\,2^{1/4} + c\,2^{1/2} + d\,2^{3/2} \;\middle|\; a, b, c, d \in \mathbb{Q}\right\}$$

25. What can you say about the order of the splitting field of $x^5+x^4+1 = (x^2+x+1)(x^3+x+1)$ over $\mathbb{Z}_2$?

Let α be a root of $x^2 + x + 1$, that is, $\alpha = x + \langle x^2 + x + 1\rangle$ in $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. So

$$\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}$$

and the multiplication table is

	α	$1+\alpha$
α	$1+\alpha$	1
$1+\alpha$	1	α

Here is how you get this, $\alpha^2 = x^2+\langle x^2+x+1\rangle$, $(\alpha+1)^2 = \alpha^2+1$ (Recall that $(a+b)^2 = a^2+b^2$ here.), and $\alpha(1 + \alpha) = \alpha^2 + \alpha$. First we compute α^2:

$$\begin{array}{rl} & 1 \\ x^2 \!\!\!& \overline{)\, x^2 + x + 1} \\ & \underline{x^2} \\ & \qquad x + 1 \end{array}$$

So $x^2 = x + 1 \pmod{x^2 + x + 1}$ so $\alpha^2 = \alpha + 1$. Hence $(\alpha + 1)^2 = \alpha^2 + 1 = \alpha + 2 = \alpha$ and $\alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1 = 1$.

We know that if $g(x) = x^3 - x + 1$ factored in $\mathbb{Z}_2(\alpha)$, then there must be one linear factor and hence a root in $\mathbb{Z}_2(\alpha)$, but we can check that this is not the case.

$$g(\alpha) = \alpha^3 + \alpha + 1 = \alpha^2\alpha + \alpha^2 = \alpha^2(\alpha + 1) = (\alpha + 1)^2 = \alpha \neq 0$$

and

$$g(\alpha + 1) = (\alpha + 1)^3 + (\alpha + 1) + 1 = (\alpha + 1)^2(\alpha + 1) + \alpha = \alpha(\alpha + 1) + \alpha = 1 + \alpha \neq 0$$

We already know that $g(0)$ and $g(1)$ are not 0. So we see that $g(x)$ is still irreducible over $\mathbb{Z}_2(\alpha)$. Let β be a root of $g(x)$, that is, $\beta = x + \langle g(x)\rangle$ in $\mathbb{Z}_2(\alpha)$. Then $[\mathbb{Z}_2(\alpha, \beta) : \mathbb{Z}_2(\alpha)] = 3$ and hence $|\mathbb{Z}_2(\alpha,\beta)| = 4^3 = 64$. Notice $[\mathbb{Z}_2(\alpha,\beta):\mathbb{Z}_2] = [\mathbb{Z}_2(\alpha,\beta):\mathbb{Z}_2(\alpha)][\mathbb{Z}_2(\alpha):\mathbb{Z}_2] = 3\cdot 2 = 6$ and so $\mathbb{Z}_2(\alpha,\beta) = 2^6 = 64$.

Now $\mathbb{Z}_2(\alpha,\beta) = \mathbb{Z}_2(\alpha)(\beta) = \mathbb{Z}_2(\alpha)(\beta)$ and

$$\mathbb{Z}_2(\alpha)(\beta) = \{a_0 + a_1\beta + a_2\beta^2 \bigm| a_i \in \mathbb{Z}_2(\alpha)\}$$

whereas

$$\mathbb{Z}_2(\beta)(\alpha) = \{a_0 + a_1\alpha \mid a_i \in \mathbb{Z}_2(\beta)\}$$

In either case, we have that a typical element of $\mathbb{Z}_2(\alpha,\beta)$ has the form

$$\begin{aligned}(a_0 + a_1\beta + a_2\beta^2) + (b_0 + b_1\beta + b_2\beta^2)\alpha &= a_0 + b_0\alpha + a_1\beta + b_1\beta\alpha + a_2\beta^2 + b_2\alpha\beta^2 \\ &= c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta + c_4\beta^2 + c_5\alpha\beta^2\end{aligned}$$

where $c_i \in \mathbb{Z}_2$.

36. Find the splitting field for $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$ over $\mathbb{Z}_3$.

Let α be a root for $x^2 + x + 2$, the elements of $\mathbb{Z}_3(\alpha)$ are of the form $a_0 + a_1\alpha$ and these are

$$0, 1, 2, \alpha, 2\alpha, 1+\alpha, 1+2\alpha, 2+\alpha, 2+2\alpha$$

Note that $\alpha^2 = -\alpha - 1 = 2 + 2\alpha$ with this, we can compute all other multiples. Let's check the status of $g(x) = x^2 + 2x + 1$

$$g(\alpha) = \alpha^2 + 2\alpha + 1 = 2 + 2\alpha + \alpha + 1 = 0$$

So $g(x)$ already has a root in $\mathbb{Z}_3(\alpha)$ and hence splits. So the splitting field of $x^4 + 1$ is $\mathbb{Z}_3(\alpha)$.

Note Not the differences between (25) and (36). When doing iterated extensions, what happens depends on whether the roots from one extension are already roots of a future extension.

37. This is sort of stated poorly. Obviously, if there is smallest field containing F and $a_1, \dots, a_n$, then

$$\bigcap\{E \mid F \subseteq E \text{ and } \{a_1, \dots, a_n\} \subset E\}$$

must be this smallest field, by definition of "smallest":)

The point is that the intersections of fields is a field; this is easy.

43. Let $F = \mathbb{Z}_p(t)$ and $f(x) = x^p - t$. Show that $f(x)$ is irreducible and has multiple roots.

$f'(x) = px^{p-1} = 0$ since F has characteristic p. Thus $f(x)$ and $f'(x)$ do have a common factor in $F[x]$, namely $f(x)$. Thus $f(x)$ has repeated roots.

By exercise (15) above, $f(x)$ is irreducible unless it splits in F. It $f(x)$ splits over F, then $t = \alpha^p = (p(t)/q(t))^p$ for some $p(t), q(t) \in \mathbb{Z}_p[t]$ with $q(t) \neq 0$ and

$$t(a_0 + a_1 t + \cdots + a_n t^n)^p = (b_0 + b_1 t + \cdots + b_m t^m)^p$$

hence $\deg(LHS) = np + 1 = mp = \deg(RHS)$, which absurd. So $f(x)$ is irreducible over F.

44. Let $f(x)$ be an irreducible polynomial over a field F. Prove that the number of distinct zeros of $f(x)$ in a splitting field divides $\deg f(x)$.

If the characteristic of F is 0, then there are $\deg(f(x))$ distinct roots. If $\mathrm{char}(F) = p$, then $f(x) = (x-a_1)^m \cdots (x-a_k)^m$ where $km = \deg(f)$. This follows from the corollary to Theorem 19.9.

47. What is the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}(\sqrt[3]{2})$? What is the splitting field over $\mathbb{Q}(\sqrt{3}i)$?

We know that the splitting field of $f(x)$ is $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. So

$$E = \mathbb{Q}(\sqrt[3]{2})(\omega) = \mathbb{Q}(\sqrt[3]{2})(\sqrt{3}i) = \mathbb{Q}(\sqrt{3}i)(\sqrt[3]{2})$$