An Introduction to Galois Theory
Solutions to the exercises

[30/06/2019]

Solutions for Exercises on Chapter 1

1.1 Clearly $\{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\} \subseteq \{n \in \mathbb{Z} : n > 0 \text{ and } n1 = 0\}$. If $0 < n \in \mathbb{Z}$ and $n1 = 0$, then for every $r \in R$,

$$nr = \underbrace{r + \cdots + r}_{n} = (\underbrace{1 + \cdots + 1}_{n})r = (n1)r = 0r = 0,$$

so

$$\{n \in \mathbb{Z} : n > 0 \text{ and } n1 = 0\} \subseteq \{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\}.$$

Hence these sets are in fact equal. When $\operatorname{char} R = p > 0$ they must both be non-empty. Now by definition of characteristic,

$$\operatorname{char} R = \min\{n \in \mathbb{Z} : n > 0 \text{ and } n1 = 0\} = \min\{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\}.$$

1.2 (a) Let $u, v \in S$ and suppose that $uv = 0$; then $u = 0$ or $v = 0$ since $u, v \in R$ and R is an integral domain. Consider the unit homomorphisms $\eta\colon \mathbb{Z} \longrightarrow R$ and $\eta'\colon \mathbb{Z} \longrightarrow S$. Then for $n \in \mathbb{Z}$, $\eta'(n) = \eta(n)$, so $\ker \eta' = \ker \eta$ and therefore $\operatorname{char} S = \operatorname{char} R$.
(b) $\mathbb{Q}$ is a field and $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring which is not a field.

1.3 (a) For any subring $R \subseteq \mathbb{C}$, R is an integral domain with characteristic subring $\mathbb{Z}$ and $\operatorname{char} R = 0$.
(b) The characteristic subring of $A[X]$ is the same as that of A and $\operatorname{char} A[X] = \operatorname{char} A$. $A[X]$ is an integral domain if and only if A is an integral domain.
(c) If we identify A with the subring of scalar matrices in $\operatorname{Mat}_n(A)$, then the characteristic subring of $\operatorname{Mat}_n(A)$ is the same as that of A and $\operatorname{char} \operatorname{Mat}_n(A) = \operatorname{char} A$. If $n > 1$ then $\operatorname{Mat}_n(A)$ is not commutative, in any case it always has zero-divisors since any singular matrix is a zero-divisor.

1.4 The main thing to check is that $\varphi(u + v) = \varphi(u) + \varphi(v)$ which is a consequence of the Idiot's Binomial Theorem. For $R = \mathbb{F}_p[X]$, φ is not surjective, while for $R = \mathbb{F}_p[X]/(X^2)$, φ is not injective.

1.5 (a) Recall from the Isomorphism Theorems of basic Ring Theory that $\varphi^{-1}Q \lhd R$; we need to show it is a prime ideal. Suppose that $u, v \in R$ with $uv \in \varphi^{-1}Q$; then $\varphi(u)\varphi(v) = \varphi(uv) \in Q$ and so $\varphi(u) \in Q$ or $\varphi(v) \in Q$, hence $u \in \varphi^{-1}Q$ or $v \in \varphi^{-1}Q$.
(b) Consider the inclusion function $\operatorname{inc}\colon R \longrightarrow S$; then $\operatorname{inc}^{-1} Q = Q \cap R$, so this result follows from (a).
(c) Consider $\mathbb{Z} \subseteq \mathbb{Q}$; then the zero-ideal $(0)_{\mathbb{Q}} \lhd \mathbb{Q}$ has $(0)_{\mathbb{Q}} \cap \mathbb{Z} = (0)_{\mathbb{Z}} \lhd \mathbb{Z}$ but this is not maximal in $\mathbb{Z}$ since for any prime $p > 0$, $(p)_{\mathbb{Z}} \lhd \mathbb{Z}$ is a (maximal) ideal that properly contains $(0)_{\mathbb{Z}}$.
(d) We have $P \subseteq Q \cap R \lhd R$ with $P \lhd R$ maximal; so $P \subseteq Q \cap R$. In fact Q only needs to be a proper ideal of S for this argument to work.

1.6 The only proper ideal of $\Bbbk$ is the zero ideal (0), so $\ker \varphi = (0)$.

1.7 (a) Addition and multiplication follow from the obvious formulae

$$(u_1 + v_1 i) + (u_2 + v_2 i) = (u_1 + u_2) + (v_1 + v_2)i, \quad (u_1 + v_1 i)(u_2 + v_2 i) = (u_1 u_2 - v_1 v_2) + (u_1 v_2 + u_2 v_1)i,$$

with $\mathbb{Z}[i]$ and $\mathbb{Q}[i]$ both closed under these operations and containing $1 = 1 + 0i$ as a unity, so they are subrings of the field $\mathbb{C}$; by Qu. 1.1, they are both integral domains. To see that $\mathbb{Q}[i]$ is a field, notice that if $u + vi \neq 0$ with $u, v \in \mathbb{Q}$,

$$(u - vi)(u + vi) = (u + vi)(u - vi) = u^2 + v^2 \neq 0,$$

so

$$\frac{u}{u^2 + v^2} + \frac{v}{u^2 + v^2}\, i \in \mathbb{Q}(i)$$

is the inverse of $u + vi$. Hence every non-zero element of $\mathbb{Q}[i]$ has an inverse, therefore $\mathbb{Q}[i]$ is a field.
(b) & (c) The crucial point is that every element of $\mathbb{Q}[i]$ can be written as $\dfrac{1}{n}(u + vi)$ with $n, u, v \in \mathbb{Z}$ and $n \neq 0$. Then

$$\operatorname{inc}_*\left(\frac{(u + vi)}{n}\right) = \operatorname{inc}_*\left(\frac{(u + vi)}{n + 0i}\right) = \frac{1}{n}(u + vi),$$

so the latter element is in the image of inc_* which must therefore be a surjection.

1.8 (a) Existence and uniqueness of such an $\psi_{a,b}$ follow from the Homomorphism Extension Property 1.22 and its effect on $f(X) = \sum_{i=0}^{n} r_i X^i \in R[X]$ where $r_i \in R$ is

$$\psi_{a,b}(f(X)) = f(aX+b) = \sum_{i=0}^{n} r_i (aX+b)^i.$$

We have

$$\psi_{a,b} \circ \psi_{c,d}(X) = \psi_{a,b}(cX+d) = c(aX+b)+d = caX + (cb+d) = \psi_{ca,cb+d}(X).$$

By the uniqueness part of the Homomorphism Extension Property, we have $\psi_{a,b} \circ \psi_{c,d} = \psi_{ca,cb+d}$.
If a is a unit then $\psi_{a^{-1},-ba^{-1}} \colon R[X] \longrightarrow R[X]$ has the property that $\psi_{a^{-1},-ba^{-1}}(aX+b) = X$ and $\psi_{a,b}(a^{-1}X - ba^{-1}) = X$, so by the uniqueness part of the Homomorphism Extension Property,

$$\psi_{a,b} \circ \psi_{a^{-1},-ba^{-1}} = \mathrm{id} = \psi_{a^{-1},-ba^{-1}} \circ \psi_{a,b}.$$

Therefore these are inverse isomorphisms, $\psi_{a^{-1},-ba^{-1}} = \psi_{a,b}^{-1}$.
(b) (i) If $f(X) = \sum_{i=0}^{n} c_i X^i \in \Bbbk[X]$ with $c_i \in \Bbbk$ and $c_n \neq 0$, then $\deg f(X) = n$. Now

$$\begin{aligned}\psi_{a,b}(f(X)) &= \sum_{i=0}^{n} c_i (aX+b)^i \\ &= c_n a^n X^n + \text{terms of lower degrees in } X.\end{aligned}$$

Since $c_n a^n \neq 0$, this shows that $\deg \psi_{a,b}(f(X)) = \deg f(X)$.
(ii) Suppose that $\psi_{a,b}(p(X)) \mid g(X)h(X)$ for $g(X), h(X) \in \Bbbk[X]$. Let $k(X) \in \Bbbk[X]$ satisfy $g(X)h(X) = k(X)\psi_{a,b}(p(X))$. Since $\psi_{a,b}$ is an isomorphism, we have

$$\psi_{a,b}^{-1}(g(X))\psi_{a,b}^{-1}(h(X)) = \psi_{a,b}^{-1}(k(X))p(X)$$

and as $p(X)$ is prime, $p(X) \mid \psi_{a,b}^{-1}(g(X))$ or $p(X) \mid \psi_{a,b}^{-1}(h(X))$. Hence $\psi_{a,b}(p(X)) \mid g(X)$ or $\psi_{a,b}(p(X)) \mid h(X)$ and so $\psi_{a,b}(p(X))$ is prime.
(iii) This follows from (ii) and Proposition 1.30.

1.9 (a) Addition and multiplication are given by the usual formulae

$$(\sum_{k=0}^{\infty} a_k X^k) + (\sum_{k=0}^{\infty} b_k X^k) = \sum_{k=0}^{\infty} (a_k + b_k) X^k, \quad (\sum_{k=0}^{\infty} a_k X^k)(\sum_{k=0}^{\infty} b_k X^k) = \sum_{k=0}^{\infty} (\sum_{\ell=0}^{k} a_\ell b_{k-\ell}) X^k.$$

Clearly $\Bbbk[X] \subseteq \Bbbk[[X]]$ is a subring. Given two *non-zero* elements $a, b \in \Bbbk[[X]]$ we may write

$$a = \sum_{k=k_0}^{\infty} a_k X^k, \quad b = \sum_{\ell_0}^{\infty} b_\ell X^\ell$$

with $a_{k_0} \neq 0 \neq b_{\ell_0}$. Then the lowest degree term in ab is $a_{k_0} b_{\ell_0} X^{k_0+\ell_0}$ with $a_{k_0} b_{\ell_0} \neq 0$. Hence $ab \neq 0$. So $\Bbbk[[X]]$ is an integral domain.
(b) Let $a = \sum_{k=0}^{\infty} a_k X^k \in \Bbbk[[X]]$. Then a has an inverse in $\Bbbk[[X]]$ only if there is a $b = \sum_{k=0}^{\infty} b_\ell X^\ell \in \Bbbk[[X]]$ with $ab = 1$, in particular this forces $a_0 \neq 0$ since otherwise the lowest term in X in ab would be of degree greater than 0. Conversely, if $a_0 \neq 0$, then we can inductively solve the system of equations

$$a_0 b_0 = 1, \qquad \sum_{\ell=0}^{n} a_\ell b_{n-\ell} = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_n = 0 \quad (n \geqslant 1),$$

to ensure that $ab = 1$.
(c) We can define make the set $\Bbbk((X))$ of all such finite tailed Laurent series into a ring with addition

and multiplication defined by

$$(\sum_{k=k_1}^{\infty} a_k X^k) + (\sum_{k=k_2}^{\infty} b_k X^k) = \sum_{k=\min\{k_1,k_2\}}^{\infty} (a_k + b_k) X^k,$$

$$(\sum_{k=k_0}^{\infty} a_k X^k)(\sum_{\ell=\ell_0}^{\infty} b_\ell X^\ell) = \sum_{k=\min\{k_0,\ell_0\}}^{\infty} (\sum_{j=0}^{k} a_\ell b_{k-j}) X^k.$$

Clearly $\Bbbk[[X]] \subseteq \Bbbk((X))$ is a subring. Notice that every element $\sum_{k=k_0}^{\infty} a_k X^k \in \Bbbk((X))$ with $k_0 < 0$ can be written as

$$(\sum_{r=0} a_{r+k_0} X^r) X^{k_0}.$$

The inclusion $\mathrm{inc}\colon \Bbbk[[X]] \longrightarrow \Bbbk((X))$ extends to the monomorphism $\mathrm{inc}_*\colon \mathrm{Fr}(\Bbbk[[X]]) \longrightarrow \Bbbk((X))$ for which

$$\mathrm{inc}_* \left(\frac{\sum_{r=0}^{\infty} a_{r+k_0} X^r}{X^{-k_0}} \right) = (\sum_{r=0}^{\infty} a_{r+k_0} X^r) X^{k_0},$$

so inc_* is surjective.

1.10 Here $f(X) = (3X - 3)d(X) + (-9X + 7)$.

1.11 Here $f(X) = -X^3 - X^2 + X + 1$ and $d(X) = -X^3 - X$ with

$$f(X) = d(X) + (-X - X^2 + 1) = d(X) + (2X^2 + 2X + 1).$$

1.12 The reduction modulo p function

$$\rho\colon \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]; \quad \rho(f(X)) = \overline{f(X)},$$

is a ring homomorphism. If $f(X) = g(X)h(X)$ with $g(X), h(X) \in \mathbb{Z}[X]$, $\deg g(X) < \deg f(X)$ and $\deg h(X) < \deg f(X)$, then

$$\overline{f(X)} = \rho(g(X)h(X)) = \rho(g(X))\rho(h(X)) = \overline{g(X)h(X)},$$

where $\deg g(X) < \deg \overline{f(X)} = \deg f(X)$ and $\deg h(X) < \deg \overline{f(X)} = \deg f(X)$. But this is impossible since $\overline{f(X)}$ is irreducible. So $f(X)$ must be irreducible.
$X^3 - X + 1$ reduces modulo 3 to an irreducible since it has no roots modulo 3. So $X^3 - X + 1$ is irreducible.
$X^3 + 2X + 1 \equiv X^3 - X + 1 \pmod 3$ so this polynomial reduces modulo 3 to an irreducible and so is irreducible.
$X^3 + X - 1$ reduces modulo 2 to an irreducible since it has no roots modulo 2. So $X^3 + X - 1$ is irreducible.
$X^5 - X + 1$ is irreducible modulo 3 and 5 so is itself irreducible.
$X^5 + X - 1 = (X^3 + X^2 - 1)(X^2 - X + 1)$ and $5X^3 - 10X + X^2 - 2 = (5X + 1)(X^2 - 2)$ so neither of these is irreducible.

1.13 $I_1 = (X^2 + 1)$, $I_2 = (X^2 + 2)$, $I_3 = (X^2 - 2)$, $I_4 = (X - \sqrt{2})$, $I_5 = (X^2 + 2)$, $I_6 = X^2 + X + 1$.

1.14 The image is

$$\varepsilon_{\sqrt{2}}\, \mathbb{Q}[X] = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

The image of $\varepsilon_{-\sqrt{2}}$ is $\varepsilon_{-\sqrt{2}}\, \mathbb{Q}[X] = \mathbb{Q}[\sqrt{2}] = \varepsilon_{\sqrt{2}}\, \mathbb{Q}[X]$. We have

$$\ker \varepsilon_{\sqrt{2}} = \ker \varepsilon_{-\sqrt{2}} = (X^2 - 2) \lhd \mathbb{Q}[X]$$

which is a maximal ideal.

1.15 Notice that $\omega = (-1 + \sqrt{3}\, i)/2 = \zeta_3$ is a primitive 3-rd root of unity and is a root of the irreducible polynomial $X^2 + X + 1 \in \mathbb{Q}[X]$. Then

$$\varepsilon_\omega\, \mathbb{Q}[X] = \mathbb{Q}[\omega] = \{a + b\omega : a, b \in \mathbb{Q}\}, \quad \ker \varepsilon_\omega = (X^2 + X + 1) \lhd \mathbb{Q}[X],$$

where $(X^2+X+1) \lhd \mathbb{Q}[X]$ is a maximal ideal. The other complex root of X^2+X+1 is ω^2, so the evaluation homomorphism ε_{ω^2} has $\varepsilon_{\omega^2}\,\mathbb{Q}[X] = \varepsilon_\omega\,\mathbb{Q}[X]$ and $\ker \varepsilon_{\omega^2} = \ker \varepsilon_\omega$.

1.16 We have

$$\varepsilon_\alpha\,\mathbb{Q}[X] = \mathbb{Q}[\alpha] = \{a+b\alpha+c\alpha^2+d\alpha^3 : a,b,c,d \in \mathbb{Q}\}, \quad \ker \varepsilon_\alpha = (X^4-2) \lhd \mathbb{Q}[X],$$

and the latter ideal is maximal. The other complex roots of X^4-2 are $-\alpha, \alpha\,i, -\alpha\,i$ (notice that two of these are real while the other two are not). Then

$$\ker \varepsilon_{-\alpha} = \ker \varepsilon_{\alpha\,i} = \ker \varepsilon_{-\alpha\,i} = (X^4-2) \lhd \mathbb{Q}[X]$$

but although $\varepsilon_{-\alpha}\,\mathbb{Q}[X] = \mathbb{Q}[\alpha]$, we have

$$\varepsilon_{\alpha\,i}\,\mathbb{Q}[X] = \varepsilon_{-\alpha\,i}\,\mathbb{Q}[X] = \mathbb{Q}[\alpha\,i] = \{a+b\alpha\,i+c\alpha^2+d\alpha^3\,i : a,b,c,d \in \mathbb{Q}\} \neq \mathbb{Q}[\alpha],$$

so $\varepsilon_{\alpha\,i}\,\mathbb{Q}[X] \neq \varepsilon_\alpha\,\mathbb{Q}[X]$ since one of these is a subset of $\mathbb{R}$ but the other is not.

If we replace $\mathbb{Q}$ by $\mathbb{R}$, then in $\mathbb{R}[X]$,

$$X^4-2 = (X^2-\sqrt{2}\,)(X^2+\sqrt{2}\,) = (X-\sqrt[4]{2}\,)(X+\sqrt[4]{2}\,)(X^2+\sqrt{2}\,).$$

Let α be a root of X^4-2. If $\alpha = \sqrt[4]{2}$, then

$$\varepsilon_\alpha\,\mathbb{R}[X] = \mathbb{R}[\alpha] = \{a+b\alpha : a,b \in \mathbb{R}\} = \mathbb{R}, \quad \ker \varepsilon_\alpha = (X-\sqrt[4]{2}\,) \lhd \mathbb{R}[X].$$

Similarly, if $\alpha = -\sqrt[4]{2}$, then

$$\varepsilon_{-\alpha}\,\mathbb{R}[X] = \mathbb{R}[-\alpha] = \{a-b\alpha : a,b \in \mathbb{R}\} = \mathbb{R}, \quad \ker \varepsilon_{-\alpha} = (X+\sqrt[4]{2}\,) \lhd \mathbb{R}[X].$$

If $\alpha^2+2=0$, then $\alpha \notin \mathbb{R}$ and

$$\varepsilon_\alpha\,\mathbb{R}[X] = \mathbb{R}[\alpha] = \{a+b\alpha : a,b \in \mathbb{R}\} = \mathbb{C}, \quad \ker \varepsilon_\alpha = (X^2+2) \lhd \mathbb{R}[X].$$

1.17 First change variable to obtain

$$g(X) = f(X+3) = X^3-6X+4.$$

Using Cardan's method we have to solve the quadratic equation

$$U^2+4U+8=0,$$

which has roots

$$-2 \pm 2i = (\sqrt{2}\,)^3 e^{3\pi i/4}.$$

Thus we can take

$$u = \sqrt{2}\,e^{\pi i/4}\omega^r = \frac{\sqrt{2}}{\sqrt{2}}\,(1+i)\omega^r = (1+i)\omega^r \quad (r=0,1,3).$$

For the roots of $g(X)$ we obtain 2, $\sqrt{3}-1$, $-\sqrt{3}-1$, while for $f(X)$ we have 5, $\sqrt{3}+2$, $-\sqrt{3}+2$.

1.18 Work backwards with Cardan's method. For α, take

$$-\frac{q}{2} = 10, \quad \frac{27q^2+4p^3}{108} = 108,$$

so $q=-20$ and $p=6$. Thus α is a real root of $f(X) = X^3+6X-20$. Notice that 2 is a real root of this polynomial and

$$f(X) = (X-2)(X^2+2X+10),$$

where $X^2+2X+10$ has no real roots. Therefore $\alpha = 2$.
For β, take

$$-\frac{q}{2} = 1, \quad \frac{27q^2+4p^3}{108} = \frac{28}{27},$$

so $q=-2$ and $p=1$. Thus β is a real root of $g(X) = X^3+X-2$ for which 1 is also a root and

$$g(X) = (X-1)(X^2+X+2),$$

where X^2+X+2 has no real roots. Therefore $\beta = 1$.

1.19 To see that the homomorphism

$$\mathrm{Aff}_1(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk[X]); \quad A \longmapsto \alpha_{A^{-1}},$$

described in the Proof of Example 1.60 is surjective, suppose that $\varphi \in \mathrm{Aut}_{\Bbbk}(\Bbbk[X])$ is any automorphism. Let

$$\varphi(X) = a_0 + a_1X + \cdots + a_nX^n$$

with $a_i \in \Bbbk$ and $a_n \neq 0$. If $n = 0$ then $\varphi\Bbbk[X] = \Bbbk \subseteq \Bbbk[X]$ so φ would not be surjective, hence we must have $n \geqslant 1$. Suppose that show that $n > 1$. Then

$$\varphi\Bbbk[X] = \{c + 0 + c_1\varphi(X) + \cdots + c_k\varphi(X)^k : c_0, c_1, \ldots, c_k \in \Bbbk\} = \Bbbk[X].$$

But if $k > 0$ and $c_k \neq 0$ then $\deg(c + 0 + c_1\varphi(X) + \cdots + c_k\varphi(X)^k) = kn > 1$, so $X \notin \varphi\Bbbk[X]$, which gives a contradiction. So we must have $n = 1$. Therefore $\varphi(X) = a_0 + a_1X$ and so $\varphi = \alpha_A$ for some $A \in \mathrm{Aff}_1(\Bbbk)$.

1.20 Calculation.

1.21 We have

$$\deg \Phi_{20}(X) = \varphi(20) = \varphi(4)\varphi(5) = 2 \times 4 = 8$$

and

$$X^{20} - 1 = (X^{10} - 1)(X^{10} + 1) = (X^{10} - 1)(X^2 + 1)(X^8 - X^6 + X^4 - X^2 + 1).$$

Since the roots of $X^{10} - 1$ are the 10-th roots of unity, we find that

$$\Phi_{20}(X) \mid (X^2 + 1)(X^8 - X^6 + X^4 - X^2 + 1);$$

since cyclotomic polynomials are irreducible, we must have $\Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$.

1.22 (a) We have

$$X^{p^k} - 1 = (X^{p^{k-1}})^p - 1 = (X^{p^{k-1}} - 1)\Phi_p(X^{p^{k-1}}),$$

so by (1.5),

$$\prod_{0 \leqslant j \leqslant k} \Phi_{p^j}(X) = \Phi_p(X^{p^{k-1}}) \prod_{0 \leqslant j \leqslant k-1} \Phi_{p^j}(X),$$

and therefore $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$. The complex roots of $\Phi_p(X)$ are the primitive p-th roots of 1, so the roots of $\Phi_{p^k}(X)$ are their p^{k-1}-st roots which are the primitive p^k-th roots of 1.
(b) Using the formula of Equation 1.4, we have

$$\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}}) = (X^{p^{k-1}} - 1)^{p-1} + c_{p-2}(X^{p^{k-1}} - 1)^{p-2} + \cdots + c_1(X^{p^{k-1}} - 1) + c_0,$$

where $c_r \equiv 0 \pmod{p}$ and $c_0 = p$. The Idiot's Binomial Theorem gives

$$X^{p^{k-1}} - 1 \equiv (X - 1)^{p^{k-1}} \pmod{p}$$

so

$$\Phi_{p^k}(X) = (X - 1)^{(p-1)p^{k-1}} + c'_{p-2}(X - 1)^{(p-2)p^{k-1}} + \cdots + c'_1(X - 1)^{p^{k-1}} + c'_0,$$

where $c'_r \equiv 0 \pmod{p}$. In fact,

$$c'_0 = \Phi_{p^k}(1) = \Phi_p(1) = c_0 = p,$$

so the Eisenstein Test can be applied to show that $\Phi_{p^k}(X)$ is irreducible over $\mathbb{Q}$.
(c) First notice that

$$\deg \Phi_n(X) = \varphi(n) = (p_1 - 1) \cdots (p_k - 1)p_1^{r_1 - 1} \cdots p_k^{r_k - 1},$$

and

$$\deg \Phi_{p_1 \cdots p_k}(X^{p_1^{r_1 - 1} \cdots p_k^{r_k - 1}}) = \varphi(p_1 \cdots p_k)p_1^{r_1 - 1} \cdots p_k^{r_k - 1} = (p_1 - 1) \cdots (p_k - 1)p_1^{r_1 - 1} \cdots p_k^{r_k - 1},$$

so $\deg \Phi_n(X) = \deg \Phi_{p_1 \cdots p_k}(X^{p_1^{r_1 - 1} \cdots p_k^{r_k - 1}})$. Also, each root ξ of $\Phi_n(X)$,

$$(\xi^{p_1^{r_1 - 1} \cdots p_k^{r_k - 1}})^{p_1 \cdots p_k} = \xi^n = 1,$$

and no smaller power of $(\xi^{p_1^{r_1-1}\cdots p_k^{r_k-1}})$ has this property, hence $(\xi^{p_1^{r_1-1}\cdots p_k^{r_k-1}})$ is a root of $\Phi_{p_1\cdots p_k}(X)$. This shows that $\Phi_n(X) \mid \Phi_{p_1\cdots p_k}(X^{p_1^{r_1-1}\cdots p_k^{r_k-1}})$. As these are monic polynomials of the same degree they are equal.

1.23 By Theorem 1.43, $\Phi_n(X) = \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (X-\zeta_n^t)$, so

$$\begin{aligned}
\Phi_n(X^{-1}) &= \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (X^{-1}-\zeta_n^t)\\
&= X^{-\varphi(n)} \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (1-X\zeta_n^t)\\
&= X^{-\varphi(n)} \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (1-X\zeta_n^{n-t})\\
&= X^{-\varphi(n)} \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (1-X\zeta_n^{-t})\\
&= X^{-\varphi(n)} \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (\zeta_n^t-X)\\
&= (-1)^{\varphi(n)} X^{-\varphi(n)} \prod_{\substack{t=1,\dots,n-1\\ \gcd(t,n)=1}} (X-\zeta_n^t)\\
&= (-1)^{\varphi(n)} X^{-\varphi(n)} \Phi_n(X).
\end{aligned}$$

Since $2 \mid \varphi(n)$ when $n > 2$ and the result is immediate when $n = 2$, we see that desired equation always holds.

1.24 We have

$$\begin{aligned}
\zeta_n + \zeta_n^{-1} &= e^{2\pi i/n} + e^{-2\pi i/n}\\
&= (\cos(2\pi/n) + \sin(2\pi/n)\, i) + (\cos(2\pi/n) - \sin(2\pi/n)\, i) = 2\cos(2\pi/n).
\end{aligned}$$

Now we have

$$\zeta_5 + \zeta_5^{-1} = 2\cos(2\pi/5), \quad \zeta_5^2 + \zeta_5^{-2} = (\zeta_5 + \zeta_5^{-1})^2 - 2 = 4\cos^2(2\pi/5) - 2.$$

We also have $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, so

$$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0.$$

Rearranging and using the formulae $\zeta_5^4 = \zeta_5^{-1}$, $\zeta_5^3 = \zeta_5^{-2}$, we have

$$(\zeta_5^2 + \zeta_5^{-2}) + (\zeta_5 + \zeta_5^{-1}) + 1 = 0,$$

hence

$$4\cos^2(2\pi/5) + 2\cos(2\pi/5) - 1 = 0.$$

Thus a suitable polynomial is $4X^2 + 2X - 1 \in \mathbb{Q}[X]$.

1.25 (a) In $K[X]$, by the Idiot's Binomial Theorem 1.11,

$$X^p - 1 = X^p + (-1)^p = (X + (-1))^p = (X-1)^p.$$

By the Unique Factorization Property 1.33, the only root of this polynomial in K must be 1. Similarly,

$$X^{np^m} - 1 = (X^n - 1)^{p^m}$$

and the only roots of this must be n-th roots of 1.
(b) If $u \in K$ is a root of this polynomial then $u^p = a$. As in (a) we have

$$X^p - a = X^p - u^p = (X - u)^p,$$

so u is the only root in K.

Solutions for Exercises on Chapter 2

2.1 This is similar to Example 2.4.

2.2 It is obvious that $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})] \leqslant 2$; if $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})] = 1$ then $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$, say $\sqrt{q} = a + b\sqrt{p}$ for some $a, b \in \mathbb{Q}$. Then

$$q = (a + b\sqrt{p})^2 = (a^2 + b^2 p) + 2ab\sqrt{p},$$

giving the simultaneous pair of equations

$$a^2 + b^2 p = q, \quad 2ab = 0.$$

If $b = 0$ then $\sqrt{q} \in \mathbb{Q}$ which contradicts the result of Qu. 2.1. If $a = 0$ then $\sqrt{q} = b\sqrt{p}$. Writing $b = b_1/b_2$ with $b_1, b_2 \in \mathbb{Z}$ and $\gcd(b_1, b_2) = 1$, we obtain

$$b_2^2 q = b_1^2 p$$

and so $p \mid b_2$ and $q \mid b_1$. Writing $b_1 = b_1' q$ and $b_2 = b_2' q$ for suitable $b_1', b_2' \in \mathbb{Z}$, we obtain

$$(b_2')^2 p^2 q = (b_1')^2 q^2 p,$$

hence

$$(b_2')^2 p = (b_1')^2 q.$$

From this we obtain $p \mid b_1'$ and $q \mid b_2'$; but then $p \mid b_1$ as well as $p \mid b_2$, contradicting the fact that $\gcd(b_1, b_2) = 1$. So $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

2.3 Arrange the induction carefully.

2.4 Notice that if $v = \pm u$ then $b = v^2 = u^2 = a$ which is impossible; so $v \neq \pm u$. Then

$$u - v = \frac{(u-v)(u+v)}{u+v} = \frac{u^2 - v^2}{u+v} = \frac{a-b}{u+v} \in K(u+v).$$

Hence

$$u = \frac{1}{2}\left((u+v) + (u-v)\right) \in K(u+v), \quad v = \frac{1}{2}\left((u+v) - (u-v)\right) \in K(u+v).$$

So $K(u,v) \leqslant K(u+v) \leqslant K(u,v)$ and therefore $K(u+v) = K(u,v)$.

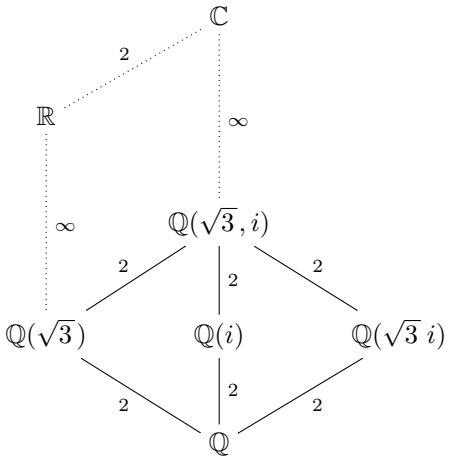
2.5 Since $1, i$ span the $\mathbb{Q}$-vector space $\mathbb{Q}(i)$, we have $[\mathbb{Q}(i):\mathbb{Q}] \leqslant 2$. But also if $x, y \in \mathbb{R}$, then $x + yi = 0 \iff x = y = 0$, so $1, i$ is a basis for $\mathbb{Q}(i)$ over $\mathbb{Q}$. Hence $[\mathbb{Q}(i):\mathbb{Q}] = 2$.

2.6 First notice that $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$ (with $\mathbb{Q}$-basis $1, \sqrt{3}$) and $\mathbb{Q}(\sqrt{3}) \leqslant \mathbb{R}$. Also, $i \notin \mathbb{Q}(\sqrt{3})$ and since $i^2 + 1 = 0$, $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3})(i)$ has $[\mathbb{Q}(\sqrt{3}, i):\mathbb{Q}(\sqrt{3})] = 2$. By Theorem 2.6(ii),

$$[\mathbb{Q}(\sqrt{3}, i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i):\mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2 \times 2 = 4.$$

The following three subfields of $\mathbb{Q}(\sqrt{3}, i)$ are distinct and are extensions of $\mathbb{Q}$ having degree 2: $L_1 = \mathbb{Q}(\sqrt{3})$, $L_2 = \mathbb{Q}(i)$, $L_3 = \mathbb{Q}(\sqrt{3}\, i)$. Then $[L_r \cap L_s : \mathbb{Q}] > 1 \iff L_r \cap L_s = L_r = L_s$, so $L_r \cap L_s = \mathbb{Q}$

whenever $r \neq s$. The only real subfield amongst these is L_1.



2.7 (a) Since 5 is a prime,

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = [\mathbb{Q}[X]/(\Phi_5(X)) : \mathbb{Q}] = \varphi(5) = 5 - 1 = 4.$$

(b) We have $\zeta_5 = \cos(2\pi/5) + \sin(2\pi/5)\, i \in \mathbb{Q}(\zeta_5)$. But also $\zeta_5^{-1} \in \mathbb{Q}(\zeta_5)$ and $\zeta_5^{-1} = \cos(2\pi/5) - \sin(2\pi/5)\, i \in \mathbb{Q}(\zeta_5)$. Hence we have

$$\cos(2\pi/5) = \frac{1}{2}\left(\zeta_5 + \zeta_5^{-1}\right) \in \mathbb{Q}(\zeta_5), \quad \sin(2\pi/5)\, i = \frac{1}{2}\left(\zeta_5 - \zeta_5^{-1}\right) \in \mathbb{Q}(\zeta_5).$$

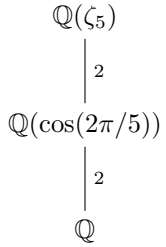
(c) This can be found by repeated use of the double angle formula

$$\cos(A + B) = \cos A \cos B - \sin A \sin B.$$

The polynomial $\mathrm{T}_n(X)$ expressing $\cos n\theta$ in terms of $\cos\theta$ is called the *n-th Chebyshev polynomial*, see Remark 6.6.
(d) For $k = 0, 1, 2, 3, 4$, $\cos(5(2k\pi/5)) = \cos(2k\pi) = 1$, so $\mathrm{T}_5(\cos 2k\pi/5) - 1 = 0$. So each of the numbers $\cos(2k\pi/5)$ is a root of the polynomial $\mathrm{T}_5(X) - 1 = (X-1)(4X^2+2X-1)^2$. For $k = 1, 2, 3, 4$, $\cos(2k\pi/5)$ is a root of $4X^2 + 2X - 1$, therefore

$$\mathbb{Q}(\cos(2\pi/5)) \cong \mathbb{Q}[X]/(4X^2 + 2X - 1), \quad [\mathbb{Q}(\cos(2k\pi/5)) : \mathbb{Q}] = 2.$$

(e)



2.8 This is similar to the previous question.

2.9 (a) If $\alpha \in \mathrm{Aut}_{\mathbb{Q}}(E_n)$ then $\alpha(2^{1/n})^n = \alpha(2) = 2$, so $\alpha(2^{1/n}) \in E_n$ is also a real n-th root of 1. If n is odd, the only possibility is $\alpha(2^{1/n}) = 2^{1/n}$, so $\alpha = \mathrm{id}$. If n is even, the possibilities are $\alpha(2^{1/n}) = \pm 2^{1/n}$. We can realize this automorphism starting with the evaluation homomorphism $\varepsilon_{2^{1/n}} \colon \mathbb{Q}[X] \longrightarrow E_n$ and precomposing with the isomorphism $\psi \colon \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]$ for which $\psi(X) = -X$ to form $\varepsilon'_{2^{1/n}} = \varepsilon_{2^{1/n}} \circ \psi$. On passing to the quotient homomorphism of $\varepsilon'_{2^{1/n}}$ we obtain an automorphism τ_n of E_n under which $\tau_n(2^{1/n}) = -2^{1/n}$.

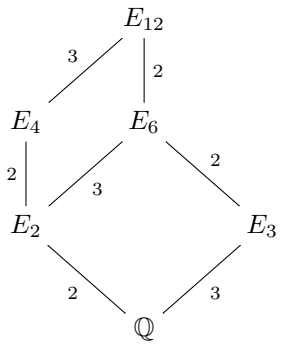
(b) Since $E \leqslant \mathbb{R}$, an automorphism $\alpha \in \mathrm{Aut}_{\mathbb{Q}}(E)$ has the effect

$$\alpha(2^{1/n}) = \begin{cases} 2^{1/n} & \text{if } n \text{ is odd,} \\ \pm 2^{1/n} & \text{if } n \text{ is even.} \end{cases}$$

If for some n we have $\alpha(2^{1/n}) = -2^{1/n}$ then

$$-2^{1/n} = \alpha(2^{1/n}) = \alpha(2^{1/2n})^2 > 0$$

since $\alpha(2^{1/2n}) \in \mathbb{R}$. This contradiction shows that $\alpha(2^{1/n}) = 2^{1/n}$ for every n, so $\alpha = \mathrm{id}$.
(c) Assuming there are only 6 such subfields, they form the following tower.



(d) This element is a root of the polynomial

$$(X - (2^{1/2} + 2^{1/3}))(X - (-2^{1/2} + 2^{1/3})) = X^2 - 2(2^{1/3})X + 2^{2/3} - 2 \in E_3[X],$$

so it is certainly an element of E_6 which is the only degree 2 extension of E_3. If $2^{1/2} + 2^{1/3} \in E_3$ then $2^{1/2} \in E_3$, which would imply $2 = [E_2 : \mathbb{Q}] \mid [E_3 : \mathbb{Q}] = 3$ which is false, so $2^{1/2} + 2^{1/3} \notin E_3$; a similar argument shows that $2^{1/2} + 2^{1/3} \notin E_2$. Writing $\omega = e^{2\pi i/3}$, $2^{1/2} + 2^{1/3}$ is a root of

$$\begin{aligned}(X - (2^{1/2} + 2^{1/3}))(X - (2^{1/2} + 2^{1/3}\omega))(X - (2^{1/2} + 2^{1/3}\omega^2)) \\ = X^3 - 3(2^{1/2})X^2 + 6X - (2 + 2(2^{1/2})) \in E_2[X],\end{aligned}$$

so it cannot lie in E_4 since $2^{1/2} + 2^{1/3} \notin E_2$ and $3 \nmid [E_4 : E_2] = 2$. So $2^{1/2} + 2^{1/3}$ is in E_6 and E_{12} and none of the others.

Solutions for Exercises on Chapter 3

3.1 Clearly, t is algebraic over K if and only if $\ker \varepsilon_t \neq (0)$, *i.e.*, (i) $\Longleftrightarrow$ (ii). By Theorem 2.9, (ii) $\Longleftrightarrow$ (iii). Hence these three conditions are indeed equivalent.

3.2 The diagrams at the bottom indicate useful subfields of the splitting fields occurring in each of these examples.

$p_1(X) = X^4 - X^2 + 1$: The polynomial $X^2 - X + 1$ has the complex roots $e^{\pm \pi i/3} = \dfrac{1 \pm \sqrt{3}\, i}{2}$, so the four roots of $p_1(X)$ are the complex square roots of these numbers, *i.e.*, $\pm e^{\pm \pi i/6}$. Explicitly these are

$$\frac{\sqrt{3}}{2} + \frac{1}{2}\, i,\ -\frac{\sqrt{3}}{2} - \frac{1}{2}\, i,\ \frac{\sqrt{3}}{2} - \frac{1}{2}\, i,\ -\frac{\sqrt{3}}{2} + \frac{1}{2}\, i.$$

The splitting field is $E = \mathbb{Q}(\sqrt{3}, i)$ and $[E : \mathbb{Q}] = 4$.

$p_2(X) = X^6 - 2$: The roots are the six complex 6-th roots of 2, *i.e.*, $\sqrt[6]{2}\, e^{2k\pi i/6} = \sqrt[6]{2}\, e^{k\pi i/3}$ for $k = 0, 1, 2, 3, 4, 5$. Explicitly, these are

$$\sqrt[6]{2},\ \frac{\sqrt[6]{2}}{2} + \frac{\sqrt[6]{2}\,\sqrt{3}}{2}\, i,\ -\frac{\sqrt[6]{2}}{2} + \frac{\sqrt[6]{2}\,\sqrt{3}}{2}\, i,\ -\sqrt[6]{2},\ -\frac{\sqrt[6]{2}}{2} - \frac{\sqrt[6]{2}\,\sqrt{3}}{2}\, i,\ \frac{\sqrt[6]{2}}{2} - \frac{\sqrt[6]{2}\,\sqrt{3}}{2}\, i.$$

The splitting field is $E = \mathbb{Q}(\sqrt[6]{2}, \sqrt{3}\, i) = \mathbb{Q}(\sqrt[6]{2})(\sqrt{3}\, i)$ which has degree $[E : \mathbb{Q}] = 12$.

$p_3(X) = X^4 + 2$: The roots are the four 4-th roots of -2, *i.e.*, $\sqrt[4]{2}\, e^{(2k+1)\pi i/4}$ for $k = 0, 1, 2, 3$. Explicitly these are

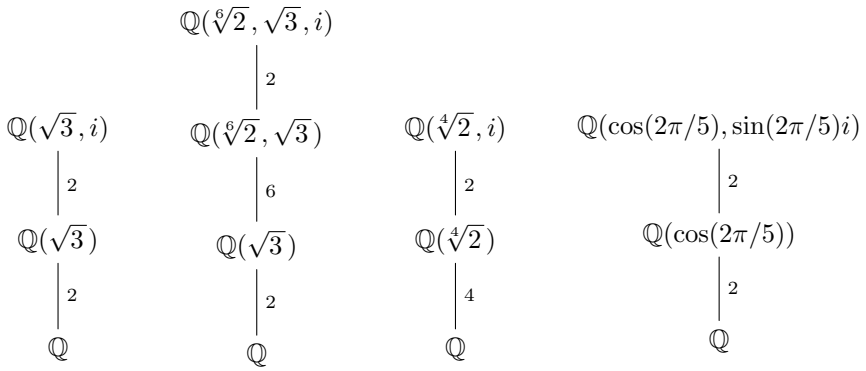
$$\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}\, i,\ -\frac{1}{\sqrt[4]{2}} + \frac{1}{\sqrt[4]{2}}\, i,\ -\frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}\, i,\ \frac{1}{\sqrt[4]{2}} - \frac{1}{\sqrt[4]{2}}\, i.$$

The splitting field is $E = \mathbb{Q}(\sqrt[4]{2}, i)$ and $[E : \mathbb{Q}] = 8$.

$p_4(X) = X^4 + 5X^3 + 10X^2 + 10X + 5$: Notice that

$$p_4(Y - 1) = Y^4 + Y^3 + Y^2 + Y + 1 = \Phi_5(Y),$$

so the splitting field of $p_4(X)$ over $\mathbb{Q}$ is the same as that of $\Phi_5(Y)$ over $\mathbb{Q}$ and this is the cyclotomic field $\mathbb{Q}(\zeta_5)$ where $\zeta_5 = \cos(2\pi/5) + \sin(2\pi/5)i$ with $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$; in fact we have $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\cos(2\pi/5), \sin(2\pi/5)i)$.



3.3 List the three roots of $X^3 - 2$ as $u_1 = \sqrt[3]{2}$, $u_2 = \sqrt[3]{2}\,\zeta_3$, $u_3 = \sqrt[3]{2}\,\zeta_3^2$. Then each automorphism $\alpha \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))$ permutes these roots, so can be identified with the unique permutation $\sigma_\alpha \in \mathrm{S}_3$ for which

$$\alpha(u_i) = u_{\sigma_\alpha(i)} \quad (i = 1, 2, 3).$$

We find that (using cycle notation for permutations)

$$\sigma_{\mathrm{id}} = \mathrm{id}, \quad \sigma_{\alpha_0} = (2\ 3), \quad \sigma_{\alpha_1} = (1\ 2\ 3), \quad \sigma_{\alpha_1'} = (1\ 2), \quad \sigma_{\alpha_2} = (1\ 3\ 2), \quad \sigma_{\alpha_2'} = (1\ 3).$$

These are the six elements of S_3, therefore $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong \mathrm{S}_3$.

3.4 Irreducibility is a consequence of the polynomial version of the Eisenstein Test 1.48. Suppose that $t \in \overline{\Bbbk(T)}$ is a root of $g(X)$; then using the Idiot's Binomial Theorem we have

$$(X-t)^p = X^p - t^p = X^p - T,$$

so t is in fact a root of multiplicity p, hence it is the only root of $g(X)$ in $\overline{\Bbbk(T)}$. This also gives the factorization of $g(X)$ into linear factors over $\overline{\Bbbk(T)}$.

3.5 $\mathbb{Q}(\sqrt{5},\sqrt{10})/\mathbb{Q}$: Here $[\mathbb{Q}(\sqrt{5},\sqrt{10}):\mathbb{Q}] = 4$ and the element $\sqrt{5}+\sqrt{10}$ has degree 4 with minimal polynomial $X^4 - 30X^2 + 25$ which has roots $\pm\sqrt{5} \pm \sqrt{10}$.
$\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$: Here $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = 4$ and the element $\sqrt{2}+i$ has degree 4 with minimal polynomial $X^4 - 2X^2 + 9$ which has roots $\pm\sqrt{2} \pm i$.
$\mathbb{Q}(\sqrt{3},i)/\mathbb{Q}$: Here $[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}] = 4$ and the element $\sqrt{3}+i$ has degree 4 with minimal polynomial $X^4 - 4X^2 + 16$ which has roots $\pm\sqrt{3} \pm i$.
$\mathbb{Q}(\sqrt[4]{3},i)/\mathbb{Q}$: Here $[\mathbb{Q}(\sqrt[4]{3},i):\mathbb{Q}] = 8$ and the element $\sqrt[4]{3}+i$ has degree 8 with minimal polynomial $X^8 + 4X^6 + 40X^2 + 4$ which has roots $\pm\sqrt[4]{3} \pm i$ and $\pm\sqrt[4]{3}\,i \pm i$.

3.6 The induction is straightforward. Here is the argument that $K(u,v)/K$ is simple. We assume that K is infinite since otherwise the result will be proved in Proposition 5.16.

Consider the subfields $K(u+tv) \leqslant K(u,v)$ with $t \in K$. Then there are only finitely many of these, so there must be $s,t \in K$ such that $s \neq t$ and $K(u+sv) = K(u+tv)$. Then

$$(s-t)v = (u+sv) - (u+tv) \in K(u+tv),$$

hence $v \in K(u+tv)$. This implies that

$$u = (u+tv) - tv \in K(u+tv),$$

hence $K(u,v) \leqslant K(u+tv) \leqslant K(u,v)$ and so $K(u,v) = K(u+tv)$.

3.7 If E/K is a quadratic extension then for any $u \in E - K$ we have $1 < [K(u):K] \leqslant 2$, so $[K(u):K] = 2 = [E:K]$ and therefore $K(u) = E$. Then $\mathrm{minpoly}_{K,u}(X)$ must factor into linear factors over E, so both its roots in $\overline{K}$ lie in E. This shows that E is normal over K.

The example $\mathbb{F}_2(Z)/\mathbb{F}_2(Z^2)$ is not separable since $X^2 - Z^2 \in \mathbb{F}_2(Z^2)[X]$ is irreducible but not separable (see Qu. 3.4). If $\mathrm{char}\, K \neq 2$ then all quadratic polynomials over K are separable.

3.8 Let $E \leqslant \mathbb{C}$ be a splitting subfield for $f(X)$ over $\mathbb{Q}$. Then if $v \in \mathbb{C}$ is a non-real root of $f(X)$ we have $v \notin \mathbb{Q}(u)$, so $f(X)$ does not split over $\mathbb{Q}(u)$ even though it has a root in this field. This means that there is a monomorphism $\varphi \in \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(u),\mathbb{C}) = \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(u),\overline{\mathbb{Q}})$ for which $\varphi(u) = v$, hence $\varphi\mathbb{Q}(u) \neq \mathbb{Q}(u)$ and so $\mathbb{Q}(u)/\mathbb{Q}$ is not normal.

Solutions for Exercises on Chapter 4

4.1 By Theorem 3.80 we know that splitting fields are always normal, so it is only necessary to show that the splitting field E of $p(X)$ over K is separable over K. Since E is obtained by repeatedly adjoining roots of $p(X)$, the result follows from Proposition 3.73 together with the fact that if $L/K \leqslant E/K$ is separable and $v \in E$ is a root of $p(X)$, then $L(v)/K$ is separable.

4.2 (a) Suppose that $f(X) = c_3X^3 + c_2X^2 + c_1X + c_4$ with $c_3 \neq 0$. Then

$$f(uX+v) = \\ c_3u^3X^3 + (3c_3vu^2 + c_2u^2)X^2 + (3c_3uv^2 + c_1u + 2c_2uv)X + (c_3v^3 + c_4 + c_1v + c_2v^2),$$

so if we take u to be any cube root of c_3 and $u = -c_2/3c_3$ then $f(uX+v)$ has the desired form. Notice that $v \in K(u)$ and then $f(uX+v) \in K(u)$, so provided that we can find a cube root of $1/c_3$ in K, we have $f(uX+v) \in K$.
(b) Viewing $\mathrm{Gal}(E/K)$ as a subgroup of S_3, by Theorem 4.8 we know that 3 divides $|\mathrm{Gal}(E/K)|$; but the only subgroups of S_3 with this property are S_3 and A_3.
(c) This is a tedious calculation! See Section 4.7 for the rest of this question.

4.3 If a/b is a rational root of $f(X)$, we may assume that $\gcd(a,b) = 1$. Now $a^3 - 3ab^2 + b^3 = 0$, which easily implies that $a, b = \pm 1$; but 1 is certainly not a root. Hence there are no rational roots and so no proper rational factors. By the formula following Proposition 4.25, the discriminant of $f(X)$ is

$$\Delta = -27 - 4(-3)^3 = 81 = 9^2.$$

If the distinct roots of $f(X)$ in $\mathbb{C}$ are u, v, w, the splitting subfield $K(v,w) = \mathbb{Q}(u,v,w) \leqslant \mathbb{C}$ satisfies $3 \mid [\mathbb{Q}(u,v,w) : \mathbb{Q}]$ and $[\mathbb{Q}(u,v,w) : \mathbb{Q}] \mid 3! = 6$. The Galois group $\mathrm{Gal}(\mathbb{Q}(u,v,w)/\mathbb{Q})$ is a subgroup of S_3 (viewed as the permutation group of $\{u,v,w\}$). Since the discriminant is a square in $\mathbb{Q}$, Proposition 4.26 implies that $\mathrm{Gal}(\mathbb{Q}(u,v,w)/\mathbb{Q}) \leqslant \mathrm{A}_3 \cong \mathbb{Z}/3$. So $|\mathrm{Gal}(\mathbb{Q}(u,v,w))/\mathbb{Q})| = 3$ and $\mathrm{Gal}(\mathbb{Q}(u,v,w))$ is cyclic of order 3 whose generator is a 3-cycle which cyclically permutes u, v, w.

4.4 (a) This should be a familiar result.
(b) The centre of D_8 is $\langle \alpha^2 \rangle$ which has order 2, and there are three normal subgroups of order 4, namely

$$\langle \alpha \rangle = \{\iota, \alpha, \alpha^2, \alpha^3\}, \quad \langle \alpha^2, \beta \rangle = \{\iota, \alpha^2, \beta, \beta\alpha^2\}, \quad \langle \alpha^2, \beta\alpha \rangle = \{\iota, \alpha^2, \beta\alpha, \beta\alpha^3\}.$$

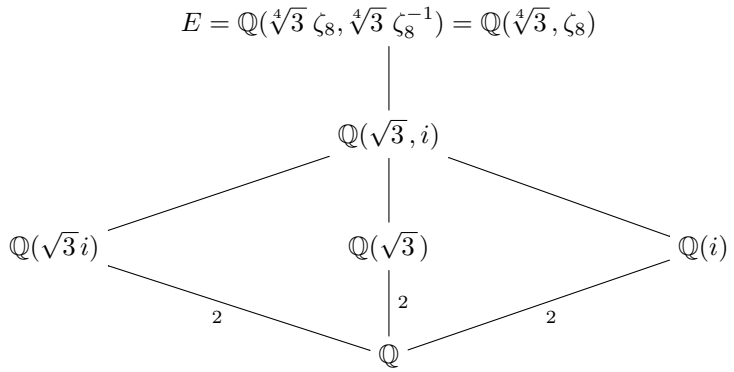
Notice that there are also four non-normal subgroups of order 2,

$$\langle \beta \rangle = \{\iota, \beta\}, \quad \langle \beta\alpha \rangle = \{\iota, \beta\alpha\}, \quad \langle \beta\alpha^2 \rangle = \{\iota, \beta\alpha^2\}, \quad \langle \beta\alpha^3 \rangle = \{\iota, \beta\alpha^3\}.$$

4.5 This is an example of case (iii) of Kaplansky's Theorem and we use the notation of the proof. The discriminant here is $\delta^2 = -12$, so we can take $\delta = 2\sqrt{3}\,i$. The roots of $X^2 + 3$ are $\pm\sqrt{3}\,i$, so we may assume

$$u = \sqrt[4]{3}\,\zeta_8 = \frac{\sqrt{2}\,\sqrt[4]{3}}{2}(1+i), \quad v = \sqrt[4]{3}\,\zeta_8^{-1} = \frac{\sqrt{2}\,\sqrt[4]{3}}{2}(1-i),$$

where as usual $\zeta_8 = e^{2\pi i/8} = (1+i)/\sqrt{2}$. Hence we have $uv = \sqrt{3}$ and $uv\delta = 6i$. This gives the diagram of subfields of E



Then α is the restriction of complex conjugation to E, while $\beta(\sqrt{3}\,i) = \sqrt{3}\,i$ and $\beta(\sqrt{3}\,) = -\sqrt{3}$, hence also $\beta(i) = -i$. Using the choices of the proof, we have

$$\beta(\sqrt[4]{3}\,\zeta_8) = -\sqrt[4]{3}\,\zeta_8, \quad \beta(\sqrt[4]{3}\,\zeta_8^{-1}) = \beta(-\sqrt[4]{3}\,\zeta_8 i) = -\sqrt[4]{3}\,\zeta_8 i.$$

The effects of σ and γ on the four roots $\sqrt[4]{3}\,\zeta_8, \sqrt[4]{3}\,\zeta_8^{-1}, -\sqrt[4]{3}\,\zeta_8, -\sqrt[4]{3}\,\zeta_8^{-1}$ of $f(X)$ are given in permutation notation by $\sigma = (1\ 4\ 3\ 2)$ and $\alpha = (1\ 2)(3\ 4)$, and these generate a dihedral subgroup of S_4. Using the previous question (but beware that the notation there is inconsistent with that of the present situation!) we have the normal subgroups

$$\langle \sigma^2 \rangle, \quad \langle \sigma \rangle, \quad \langle \sigma^2, \alpha \rangle, \quad \langle \sigma^2, \alpha\sigma \rangle,$$

and these have fixed fields

$$E^{\langle \sigma^2 \rangle} = \mathbb{Q}(\sqrt{3}, i), \quad E^{\langle \sigma \rangle} = \mathbb{Q}(i), \quad E^{\langle \sigma^2, \alpha \rangle} = \mathbb{Q}(\sqrt{3}\,), \quad E^{\langle \sigma^2, \alpha\sigma \rangle} = \mathbb{Q}(\sqrt{3}\,i),$$

each of which is a normal extension of $\mathbb{Q}$.

4.6 $\mathbb{Q}(X^3 - 10)/\mathbb{Q}$: This is similar to Example 4.20, with splitting field $\mathbb{Q}(\sqrt[3]{10}\,, \zeta_3)$ and Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{10}\,, \zeta_3)/\mathbb{Q}) \cong \mathrm{S}_3$.
$\mathbb{Q}(\sqrt{2}\,)(X^3 - 10)/\mathbb{Q}(\sqrt{2}\,)$: The splitting field is $\mathbb{Q}(\sqrt{2}\,, \sqrt[3]{10}\,, \zeta_3)$, $[\mathbb{Q}(\sqrt{2}\,, \sqrt[3]{10}\,) : \mathbb{Q}(\sqrt{2}\,)] = 3$ and

$$\mathbb{Q}(\sqrt{2}\,, \sqrt[3]{10}\,) \leqslant \mathbb{Q}(\sqrt{2}\,, \sqrt[3]{10}\,, \zeta_3).$$

Since ζ_3 is not real, $[\mathbb{Q}(\sqrt{2}\,, \sqrt[3]{10}\,, \zeta_3) : \mathbb{Q}(\sqrt{2}\,)] = 6$. The Galois group is isomorphic to S_3.
$\mathbb{Q}(\sqrt{3}\,i)(X^3 - 10)/\mathbb{Q}(\sqrt{3}\,i)$: Here $\mathbb{Q}(\sqrt{3}\,i) = \mathbb{Q}(\zeta_3)$, with $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. The splitting field is $\mathbb{Q}(\sqrt[3]{10}\,, \zeta_3)$ and $[\mathbb{Q}(\sqrt[3]{10}\,, \zeta_3) : \mathbb{Q}(\zeta_3)] = 3$, hence $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{10}\,, \zeta_3)/\mathbb{Q}(\zeta_3)) \cong \mathbb{Z}/3$ with generator σ for which $\sigma(\sqrt[3]{10}\,) = \sqrt[3]{10}\,\zeta_3$.
$\mathbb{Q}(\sqrt{23}\,i)(X^3 - X - 1)/\mathbb{Q}(\sqrt{23}\,i)$: First note that $X^3 - X - 1 \in \mathbb{Z}[X]$ must be irreducible since its reduction modulo 2, $X^3 + X + 1 \in \mathbb{F}_2[X]$, has no root in $\mathbb{F}_2$ and hence has no linear factor (see Qu. 1.10). To proceed further we can use the ideas of Qu. 4.2 above (see also Section 4.7). The discriminant of the polynomial $X^3 - X - 1$ is $\Delta = -23$ and so $\delta = \sqrt{23}\,i$. Then if $E = \mathbb{Q}(\sqrt{23}\,i)(X^3 - X - 1)$ is the splitting field of $X^3 - X - 1$ over $\mathbb{Q}$, $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{S}_3$ and $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{23}\,i)) \cong \mathrm{A}_3$.
$K(X^3 - X - 1)/K$ for $K = \mathbb{Q}$, $\mathbb{Q}(\sqrt{5}\,)$, $\mathbb{Q}(\sqrt{5}\,i)$, $\mathbb{Q}(i)$: Continuing the preceding discussion, notice that $[E \cap \mathbb{R} : \mathbb{Q}] = 3$, so $\sqrt{5} \notin E$, hence

$$\mathbb{Q}(\sqrt{5}\,)(X^3 - X - 1) = \mathbb{Q}(X^3 - X - 1)(\sqrt{5}\,)$$

and

$$[\mathbb{Q}(\sqrt{5}\,)(X^3 - X - 1) : \mathbb{Q}(\sqrt{5}\,)] = [\mathbb{Q}(X^3 - X - 1) : \mathbb{Q}] = 6,$$

hence $\mathrm{Gal}(\mathbb{Q}(\sqrt{5}\,)(X^3 - X - 1)/\mathbb{Q}(\sqrt{5}\,)) \cong \mathrm{S}_3$. Similarly, $\sqrt{5}\,i \notin E$ and $i \notin E$, hence

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{5}\,i)(X^3 - X - 1)/\mathbb{Q}(\sqrt{5}\,i)) \cong \mathrm{S}_3 \cong \mathrm{Gal}(\mathbb{Q}(i)(X^3 - X - 1)/\mathbb{Q}(i)).$$

4.7 (a) Since $\operatorname{char} K \neq 0$, $f'(X) = pX^{p-1} \neq 0$, so if $u \in L$ is any root of $f(X)$ then $f'(u) = pu^{p-1} \neq 0$. By Proposition 3.55, there are no multiple roots, hence p distinct roots. If $u, v \in L$ are distinct roots, then $(vu^{-1})^p = 1$, so $v = u\xi$ for $\xi \in K$ a p-th root of 1 with $\xi \neq 1$.
(b) If there is a root $u \notin K$, the Galois group $\operatorname{Gal}(L/K)$ acts in the following way. By Theorem 4.8, there must be an element $\gamma \in \operatorname{Gal}(L/K)$ with $\gamma(u) \neq u$. We can write $\gamma(u) = u\xi_\gamma$ where $\xi_\gamma \neq 1$ is a p-th root of 1. Since $\gamma(\xi_\gamma) = \xi_\gamma$, for $r \geqslant 1$ we have $\gamma^r(u) = u\xi_\gamma^r$, which can only equal u if $p \mid r$. So u must have at least p conjugates which are all roots of $f(X)$. Since $\deg f(X)_p$, every root of $f(X)$ is conjugate to u, so $f(X)$ must be irreducible over K.
(c) Suppose that $f(X) = g(X)h(X)$ with $g(X) \in K[X]$ monic irreducible and $0 < d = \deg g(X) < p$. Let L/K with L a splitting field for $f(X)$ over K and let $w \in L$ be a root of $g(X)$. Arguing as in (a), we know that each root of $g(X)$ has the form $w\xi$ where ξ is some p-th root of 1; moreover, L must contain p distinct p-th roots of 1. Now the constant coefficient of $g(X)$ is $g(0) = (-1)^d\xi_0 w^d \in K$ where ξ_0 is a p-th root of 1. So

$$g(0)^p = (-1)^{dp}\xi_0^p(w^p)^d = (-1)^{dp}a^d,$$

from which it follows that a^d is a p-th power in K. As $\gcd(p, d) = 1$, there are integers r, s such that $rp + sd = 1$, so we have

$$a = (a^r)^p(a^d)^s = \text{a } p\text{-th power in } K.$$

Hence if $f(X)$ is *not* irreducible in $K[X]$ it has a root in K.

4.8 If $u \in L$ is a root of $f(X)$ in an extension L/K then by the Idiot's Binomial Theorem 1.11

$$X^p - a = X^p + (-u)^p = (X - u)^p,$$

so u is the only such root in L and $f(X)$ splits over L. If $(X - u)^d \in K[X]$ for some d with $1 < d < p$ then $u^d \in K$. Since $\gcd(d, p) = 1$, there are integers r, s such that $rd + sp = 1$. Hence $(u^d)^s(u^p)^r = u$, where the left hand side is in K. This shows that $u \in K$. Hence either $f(X)$ has a root in K or it must be irreducible over K.

4.9 (a) These may be verified using standard rules for manipulating determinants, since the effect of changing the entries in the resultant is easily described in terms of elementary row operation applied to the determinant.
(b) Suppose that $h(X) = \gcd(p(X), q(X))$. The Euclidean Algorithm produces polynomials $u(X), v(X)$ with $\deg u(X) \leqslant n$ and $\deg v(X) \leqslant m$, for which $h(X) = u(X)p(X) + v(X)q(X)$.

Each step in the Euclidean algorithm has the form

$$f(X) = q(X)g(X) + r(X),$$

where $\deg r(X) < \deg g(X)$ or $r(X) = 0$. Using part (a), it is easy to see that

$$\operatorname{Res}(f(X), g(X)) = \operatorname{Res}(r(X), g(X))$$

and by repeating this we obtain either $\gcd(p(X), q(X)) = 1$ and $\operatorname{Res}(p(X), q(X)) \neq 0$, or $\gcd(p(X), q(X)) \neq 1$ and

$$\operatorname{Res}(p(X), q(X)) = \operatorname{Res}(h(X), h(X)) = 0.$$

(c) This follows from part (b) and the derivative test of Proposition 3.55.

Solutions for Exercises on Chapter 5

5.1 By Theorem 1.17, an integral domain D always admits a monomorphism into a field $j\colon D \longrightarrow F$ (*e.g.*, F can be taken to be the field of fractions of D), so any subgroup $U \leqslant D^\times$ becomes isomorphic to a subgroup $jU \leqslant F^\times$, and if U is finite so is jU. Therefore jU and U are cyclic.

5.2 The only root of X^2+1 in $\overline{\mathbb{F}}_2$ is the multiple root 1.

5.3 The field $\mathbb{F}_{p^d}[X]/(f(X))$ is an extension of $\mathbb{F}_{p^d}$ which has degree n, hence it is a finite field with p^{dn} elements, hence Proposition 5.6 implies that it is isomorphic to $\mathbb{F}_{p^{dn}}$. Since the extension $\mathbb{F}_{p^{dn}}/\mathbb{F}_{p^d}$ is normal, $\mathbb{F}_{p^{dn}}$ is a splitting field for $f(X)$ over $\mathbb{F}_{p^d}$.

5.4 (a) Here 41 is prime. Since $8 \mid (41-1)$, there is a primitive 8-th root of unity in $\mathbb{F}_{41}$. 6 is a primitive root for $\mathbb{F}_{41}$ and $6^5 \equiv 27 \bmod 41$ has order 8.
(b) Here 5 is prime $4 \mid (5-1)$, so there is a primitive 4-th root of unity in $\mathbb{F}_5^\times$, but no primitive 8-th root of unity. In fact, 2 and 3 have order 4, so these are primitive roots for $\mathbb{F}_5$. Notice that in $\mathbb{F}_5[X]$,

$$X^8-1 = (X^4-1)(X^4+1) = (X^4-1)(X^2-2)(X^2-3),$$

where the polynomials X^2-2 and X^2-3 are irreducible. Therefore $\mathbb{F}_{25}$ is the splitting field for X^8-1 over $\mathbb{F}_5$ and we have $\mathbb{F}_{25} \cong \mathbb{F}_5(u) = \mathbb{F}_5(v)$, where $u^2=2$ and $v^2=3$, so $\pm u$ and $\pm v$ are primitive 8-th roots of unity. To find an element of order 24 in $\mathbb{F}_{25}^\times$, we first find one of order 3. Consider the polynomial $X^2+X+1 \in \mathbb{F}_5[X]$; in $\overline{\mathbb{F}}_5$, this has roots which have order 3. These roots are given by $(-1 \pm w)/2$, where $w^2 = (1-4) = -3 = 2$, hence they are

$$\frac{(-1 \pm u)}{2} = -3 \pm 3u.$$

Now the elements $\pm(2 \pm 2u)u = \pm(\pm 4 + 2u) = \pm 4 \pm 2u$ all have order $8 \times 3 = 24$.
(c) Here 11 is prime and $8 \mid (121-1) = 120$, so $\mathbb{F}_{121}$ is the splitting field of X^8-1 over $\mathbb{F}_{11}$. The polynomial X^2+1 is irreducible over $\mathbb{F}_{11}$ so $\mathbb{F}_{121} = \mathbb{F}_{11}(z)$ where $z^2=-1$. Since $120 = 8 \times 3 \times 5$, it is sufficient to find elements of order 8, 3 and 5 whose product will have order 120.

Suppose that $a+bz \in \mathbb{F}_{121}$ with $a, b \in \mathbb{F}_{11}$. If this element has order 8, then $(a+bz)^2 = \pm z$. So let us solve

$$(a^2-b^2) + 2abz = z.$$

Then $2ab = 1$ and $b^2 = a^2$, hence $b = \pm a$. Now we have $2a^2 = \pm 1$ and so $a^2 = \pm 1/2 = \pm 6$. Now 6 is not a square in $\mathbb{F}_{11}$ but

$$7^2 \equiv -6 \equiv 4^2 \pmod{11},$$

so we have $a=4$, $b=\pm 4$ and $a=7$, $b=\pm 7$. Therefore the elements of order 8 in $\mathbb{F}_{121}^\times$ are $4 \pm 4z$ and $7 \pm 7z$.

By the same approach as in (b), the elements of order 3 in $\mathbb{F}_{121}$ are $(-1 \pm 5z)/2 = 5 \pm 8z$.

2 is a primitive root for $\mathbb{F}_{11}$ so $4 = 2^2$ has order 5.

Combining these we obtain the following primitive roots for $\mathbb{F}_{121}$: $7 \pm z$, $10 \pm 4z$.
(d) In $\mathbb{F}_2[X]$ we have $X^8-1 = (X-1)^8$, whose only root in $\overline{\mathbb{F}}_2$ is 1. So the splitting field is $\mathbb{F}_2$.

5.5 Notice that $\mathbb{F}_p(w)$ is a splitting field of the separable polynomial $X^{p^d-1}-1$ over $\mathbb{F}_p$, so if $w \in \mathbb{F}_{p^\ell}^\times$ then $\mathbb{F}_p(w) \leqslant \mathbb{F}_{p^\ell}$. Since $\mathbb{F}_p(w) = \mathbb{F}_{p^d}$ we have $d \leqslant \ell$; we also have $\deg_{\mathbb{F}_p} w = d$. The number of conjugates of w is d, hence each primitive root of $\mathbb{F}_{p^d}$ has d conjugates and the total number of these is the number of generators of the cyclic group $\mathbb{F}_{p^d}^\times \cong \mathbb{Z}/(p^d-1)$, *i.e.*, $\varphi(p^d-1)$. Hence $d \mid \varphi(p^d-1)$. This can also be interpreted in terms of the evident action of $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathbb{Z}/d$ on the set of all primitive roots of $\mathbb{F}_{p^d}$; each orbit has exactly d elements, so the number of orbits is $\varphi(p^d-1)/d$ which is an integer.

5.6 (a) First note that $g_a'(X) = -1$, so $g_a(X)$ is separable, hence E/K is separable. If $u \in E$ is a root of $g_a(X)$, then for $t \in \mathbb{F}_{p^d}$,

$$g_a(u+t) = (u+t)^{p^d} - (u+t) - a = (u^{p^d} - u - a) + (t^{p^d} - t) = (u^{p^d} - u - a) = 0,$$

hence $u+t$ is also a root of $g_a(X)$. This means that $E = K(u)$ since all the other roots of $g_a(X)$ lie in $K(u)$. As $g_a(X)$ is irreducible over K, $[E : K] = p^d = |\operatorname{Gal}(E/K)|$ and so the following p^d automorphisms are the elements of $\operatorname{Gal}(E/K)$:

$$\sigma_t \colon E \longrightarrow E; \quad \sigma_t(u) = u + t \qquad (t \in \mathbb{F}_{p^d}).$$

It is easy to check that for $s, t \in \mathbb{F}_{p^d}$, $\sigma_s \circ \sigma_t = \sigma_{s+t}$. Hence there is an isomorphism $\operatorname{Gal}(E/K) \cong \mathbb{F}_{p^d}$ with σ_t corresponding to $t \in \mathbb{F}_{p^d}$.

(b) If $g_a(X)$ is irreducible over K then it cannot have a root in K since its degree is greater than 1.

Conversely, suppose that $g_a(X)$ has no root in K. Then if $u \in E$ is any root of $g_a(X)$ in a splitting field over K, the other roots are the p elements $u + t \in E$ ($t \in \mathbb{F}_p$). If $u + t_0 \neq u$ is a conjugate of u with $0 \neq t_0 \in \mathbb{F}_p$, there must be an element $\tau_{t_0} \in \operatorname{Gal}(E/K)$ for which $\tau_{t_0}(u) = u + t_0$. Then $\langle \tau_{t_0} \rangle$ must be isomorphic to a non-trivial subgroup of $\mathbb{F}_p$, but this must be $\mathbb{F}_p$ since this group is simple. Hence, u must have p conjugates and so $g_a(X)$ is irreducible over K.

(c) If K is a finite field and $d > 1$ then if $g_a(X)$ were irreducible over K, then by (a), E would be finite and $\operatorname{Gal}(E/K) \cong \mathbb{F}_{p^d}$. But $\mathbb{F}_{p^d}$ is not cyclic, yet we know from Proposition 5.23 that $\operatorname{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathbb{Z}/d$ is cyclic.

5.7 (a) By Proposition 5.12, $\mathbb{F}_q^\times$ is a cyclic group. If $p = 2$ then $|\mathbb{F}_{2^d}^\times| = 2^d - 1$, which is odd, so every element of $\mathbb{F}_{2^d}^\times$ is a square; we may therefore take $\lambda_{2^d}(u) = 1$ for all $u \in \mathbb{F}_{2^d}^\times$. So now suppose that p is odd. Then $|\mathbb{F}_{p^d}^\times| = p^d - 1$, which is even. The set of squares in $\mathbb{F}_{p^d}^\times$ is the normal subgroup

$$(\mathbb{F}_{p^d}^\times)^2 = \{u^2 : u \in \mathbb{F}_{p^d}^\times\} \leqslant \mathbb{F}_{p^d}^\times$$

and it is easily seen that its quotient group has order 2, hence

$$\mathbb{F}_{p^d}^\times / (\mathbb{F}_{p^d}^\times)^2 \cong \{\pm 1\}.$$

We may use this group isomorphism to define λ_q. Clearly we have

$$\ker \lambda_q = (\mathbb{F}_{p^d}^\times)^2.$$

λ_q is surjective if and only if p is odd.

Remark: when $d = 1$, $\lambda_p(u) = \left(\dfrac{u}{p}\right)$, the *Legendre symbol* of u from Number Theory.

(b) If $u \in \Sigma_q$, then either $u = 0$ or $u \neq 0$ and $u = (\pm v)^2$ for some $v \in \mathbb{F}_q^\times$. Thus we have

$$|\Sigma_q| = 1 + \frac{(q-1)}{2} = \frac{(q+1)}{2}\,.$$

Then

$$|t - \Sigma_q| = |\Sigma_q| = \frac{(q+1)}{2}\,.$$

(c) Since $\Sigma_q \cup (t - \Sigma_q) \subseteq \mathbb{F}_q$, we have

$$q \geqslant |\Sigma_q \cup (t - \Sigma_q)| = |\Sigma_q| + |t - \Sigma_q| - |\Sigma_q \cap (t - \Sigma_q)|.$$

This implies that

$$q \geqslant (q+1) - |\Sigma_q \cap (t - \Sigma_q)|$$

and so

$$|\Sigma_q \cap (t - \Sigma_q)| \geqslant 1.$$

Thus for every $t \in \mathbb{F}_q$, there are $u, v \in \mathbb{F}_q$ (possibly 0) for which $u^2 = t - v^2$, whence $t = u^2 + v^2$.

(d) By (c), we may write $-1 = a^2 + b^2$ for some $a, b \in \mathbb{F}_q$, *i.e.*,

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

Solutions for Exercises on Chapter 6

6.1 Now when $n = 1$, $G \cong \mathbb{Z}/p$, which is abelian. Suppose that the result holds whenever $|G| = p^k$ with $k < n$. If $|G| = p^n$, recall that by Cauchy's Lemma, the centre Z of G is non-trivial. Hence G/Z has order $|G/Z| = p^k$ with $k < n$. By the inductive hypothesis, there is a normal subgroup $M \lhd G/Z$ with $|M| = p^{k-1}$. By one of the Isomorphism Theorems, there is a normal subgroup $N \lhd G$ containing Z and satisfying $N/Z = M \subseteq G/Z$. Clearly $|N| = |Z|\,|M| = p^{n-1}$. This establishes the inductive step and hence the desired result.

6.2 In this situation, for any non-zero $t \in K$, $-t \neq t$ (since otherwise $2t = 0$ and so $t = 0$). If $\zeta \in K$ is a primitive n-th root of unity, then $(-\zeta)^n = (-1)^n\zeta^n = -1$, while $(-\zeta)^{2n} = (-1)^{2n}\zeta^{2n} = 1$. Hence $-\zeta \in K$ is a primitive $2n$-th root of unity.

6.3 Write $n = 2^k p_1^{r_1} \cdots p_s^{r_s}$, where each p_j is an odd prime, $p_1 < p_2 < \cdots < p_s$, $r_j \geqslant 1$ and $k \geqslant 0$. Then

$$\varphi(n) = \varphi(2^k)\varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s}) = \varphi(2^k)(p_1 - 1)p_1^{r_1-1} \cdots (p_s - 1)p_s^{r_s-1}.$$

If $s > 0$ then $\varphi(n) \mid 4$ happens precisely when $r_1 = \cdots = r_s = 1$ and one of the following possibilities occurs:

- $p_1 = 5$, $s = 1$ and $k = 0$ (hence $n = 5$);
- $p_1 = 3$, $s = 1$ and $k = 0, 1, 2$ (hence $n = 3, 6, 12$);
- $s = 0$ and $k = 0, 1, 3$ (hence $n = 1, 2, 4, 8$).

$\mathbb{Q}(i)$: Here degree $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and clearly the four 4-th roots of unity $\pm 1, \pm i$ lie in this field. As $\varphi(5) = 4$, it has no 5-th roots of unity except 1. If it contained a 3-rd root of unity then it would contain $\sqrt{3}$ and so $\mathbb{Q}(\sqrt{3}\,, i) \leqslant \mathbb{Q}(i)$ which is impossible since $[\mathbb{Q}(\sqrt{3}\,, i) : \mathbb{Q}] = 4$. From this we see that the only roots of unity in $\mathbb{Q}(i)$ are $\pm 1, \pm i$.

$\mathbb{Q}(\sqrt{2}\,i)$: This field contains only the square roots of unity ± 1.

$\mathbb{Q}(\sqrt{3}\,i)$: This contains the six 6-th roots of unity $\pm 1, \pm\dfrac{1}{2} \pm \dfrac{\sqrt{3}}{2}\,i$.

$\mathbb{Q}(\sqrt{5}\,i)$: This field contains only the square roots of unity ± 1.

6.4 (a) We have $\varphi(24) = \varphi(8)\varphi(3) = 4 \times 2 = 8$. The elements of $\mathbb{Z}/24$ which are invertible are the residue classes modulo 24 of the numbers 1, 5, 7, 11, 13, 17, 19, 23. For each of these numbers r, the residue class modulo 24, $\overline{r}$, satisfies $\overline{r}^2 = \overline{1}$, hence these all have order 2 except $\overline{1}$ which has order 1. Since $(\mathbb{Z}/24)^\times$ is abelian, it is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. The effect of these elements on $\mathbb{Q}(\zeta_{24})$ is given by $\overline{r} \cdot \zeta_{24}^r$. Notice that $\overline{23}$ acts like complex conjugation. The effect on $\mathbb{Q}(\cos(\pi/12))$ is given by

$$\overline{r} \cdot \cos(\pi/12) = \cos(\pi r/12),$$

so in particular,

$$\overline{-r} \cdot \cos(\pi/12) = \cos(-\pi r/12) = \cos(\pi r/12) = \overline{r} \cdot \cos(\pi/12).$$

(b) This is similar to (a). We have $\varphi(20) = \varphi(4)\varphi(5) = 2 \times 4 = 8$ and the elements of $(\mathbb{Z}/20)^\times$ are the residue classes modulo 20 of the numbers 1, 3, 7, 9, 11, 13, 17, 19. This time there are elements of order 4, for instance $\overline{7}$ and $\overline{13}$. Then we have $(\mathbb{Z}/20)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/4$.

6.5 For any $n \geqslant 1$, let $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + \sin(2\pi/n)\,i$. Notice that if n is odd, then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(-\zeta_n)$ where $-\zeta_n$ is a primitive $2n$-th root of unity, so we might as well assume that n is even from now on. We also have

$$\zeta_n - \zeta_n^{-1} = 2\sin(2\pi/n)\,i \in \mathbb{Q}(\zeta_n).$$

(a) If $4 \nmid n$ then writing $n = 2k$ with k odd, we have

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(2k) = \varphi(2)\varphi(k) = \varphi(k),$$

while

$$[\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}] = \varphi(4k) = \varphi(4)\varphi(k) = 2\varphi(k).$$

Hence, $\mathbb{Q}(\zeta_n)$ cannot contain ζ_{2n} and by another simple argument it cannot contain $i = \zeta_{2n}^k$. So we see that $\sin(2\pi/n) \notin \mathbb{Q}(\zeta_n)$ in this situation. Notice that since $i = \zeta_{2n}^k$,

$$\sin(2\pi/n) = \frac{\zeta_{2n}^2 - \zeta_{2n}^{-2}}{2i} \in \mathbb{Q}(\zeta_{2n}),$$

and by Theorem 6.3,

$$\sin(2\pi/n) \in \mathbb{Q}(\zeta_{2n}) \cap \mathbb{R} = \mathbb{Q}(\cos(\pi/n)).$$

Also, we have

$$[\mathbb{Q}(\cos(\pi/n)) : \mathbb{Q}] = 2[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}],$$

hence

$$\mathbb{Q}(\cos(\pi/n)) = \mathbb{Q}(\cos(2\pi/n))(\sin(2\pi/n))$$

and

$$[\mathbb{Q}(\cos(2\pi/n))(\sin(2\pi/n)) : \mathbb{Q}(\cos(2\pi/n))] = 2,$$

with

$$\operatorname{minpoly}_{\mathbb{Q}(\cos(2\pi/n)),\sin(2\pi/n)}(X) = X^2 + \cos^2(2\pi/n) - 1.$$

If $4 \mid n$, we can write $n = 4\ell$. Then $i = \zeta_n^\ell$, so $i \in \mathbb{Q}(\zeta_n)$, whence

$$\sin(\pi/2\ell) = \sin(2\pi/n) = \frac{\zeta_n - \zeta_n^{-1}}{i} \in \mathbb{Q}(\zeta_n).$$

Clearly

$$\sin(\pi/2\ell) \in \mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\cos(2\pi/n)).$$

Consider the automorphism $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}))$ for which $\sigma(\zeta_n) = \zeta_n^{2\ell+1} = -\zeta_n$; it is easy to see that σ has order 2. Then

$$\begin{aligned}
\sigma(\cos(2\pi/n)) &= \sigma(\cos(\pi/2\ell)) = -\cos(\pi/2\ell),\\
\sigma(\cos(\pi/\ell)) &= \cos(\pi/\ell),\\
\sigma(\sin(2\pi/n)) = \sigma(\sin(\pi/2\ell)) &= \frac{-\zeta_n + \zeta_n^{-1}}{2(-\zeta_n)^\ell} = \begin{cases} \sin(\pi/2\ell) & \text{if } \ell \text{ is odd,}\\ -\sin(\pi/2\ell) & \text{if } \ell \text{ is even.}\end{cases}
\end{aligned}$$

From this we find that when ℓ is odd,

$$\mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(\cos(\pi/2\ell)) = \mathbb{Q}(\cos(\pi/\ell))(\sin(\pi/2\ell)) = \mathbb{Q}(\sin(\pi/2\ell)),$$

since $\cos(\pi/\ell) = 1 - 2\sin^2(\pi/2\ell) \in \mathbb{Q}(\sin(\pi/2\ell))$. Thus we have $[\mathbb{Q}(\sin(\pi/2\ell)) : \mathbb{Q}] = 2\varphi(\ell)$ and

$$\operatorname{Gal}(\mathbb{Q}(\sin(\pi/2\ell))/\mathbb{Q}) = \operatorname{Gal}(\mathbb{Q}(\cos(\pi/2\ell))/\mathbb{Q}) = (\mathbb{Z}/4\ell)^\times/\{\overline{1}, \overline{-1}\}.$$

Similarly, if ℓ is even,

$$[\mathbb{Q}(\cos(\pi/\ell))(\sin(\pi/2\ell)) : \mathbb{Q}(\cos(\pi/\ell))] = 2$$

and we must have

$$\mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(\cos(\pi/2\ell)) = \mathbb{Q}(\sin(\pi/2\ell))$$

with

$$\operatorname{Gal}(\mathbb{Q}(\sin(\pi/2\ell))/\mathbb{Q}) = \operatorname{Gal}(\mathbb{Q}(\cos(\pi/2\ell))/\mathbb{Q}) = (\mathbb{Z}/4\ell)^\times/\{\overline{1}, \overline{-1}\}$$

(b) We have

$$\sin^2(\pi/12) = \frac{1 - \cos(\pi/6)}{2} = \frac{2 - \sqrt{3}}{4},$$

and so

$$\sin(\pi/12) = \frac{\sqrt{2 - \sqrt{3}}}{2} = \frac{\sqrt{6} - \sqrt{2}}{4}.$$

Then

$$\mathbb{Q}(\sin(\pi/12)) = \mathbb{Q}(\sqrt{6} - \sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

and

$$\operatorname{Gal}(\mathbb{Q}(\sin(\pi/12))/\mathbb{Q})) \cong (\mathbb{Z}/4\ell)^\times/\{\overline{1}, \overline{-1}\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Here the effect of the coset of the residue class of $\overline{r} \in (\mathbb{Z}/4\ell)^\times$ is given by

$$\overline{r} \cdot \sin(\pi/12) = \frac{\zeta_{24}^r - \zeta_{24}^r}{i^r} = \sin(r\pi/12)\, i^{1-r}.$$

Explicitly we have

$$\begin{aligned}
\overline{1} \cdot \sin(\pi/12) = \overline{-1} \cdot \sin(\pi/12) &= \sin(\pi/12) = \frac{\sqrt{6}-\sqrt{2}}{4}\,,\\
\overline{5} \cdot \sin(\pi/12) = \overline{-5} \cdot \sin(\pi/12) &= \sin(5\pi/12) = \frac{\sqrt{6}+\sqrt{2}}{4}\,,\\
\overline{7} \cdot \sin(\pi/12) = \overline{-7} \cdot \sin(\pi/12) &= -\sin(7\pi/12) = \frac{-\sqrt{6}-\sqrt{2}}{4}\,,\\
\overline{11} \cdot \sin(\pi/12) = \overline{-11} \cdot \sin(\pi/12) &= -\sin(11\pi/12) = \frac{-\sqrt{6}+\sqrt{2}}{4}\,.
\end{aligned}$$

In terms of the generators $\sqrt{2}$ and $\sqrt{3}$ these act by

$$\begin{aligned}
&\overline{1} \cdot \sqrt{2} = \sqrt{2}\,, && \overline{1} \cdot \sqrt{3} = \sqrt{3}\,, && \overline{5} \cdot \sqrt{2} = -\sqrt{2}\,, && \overline{5} \cdot \sqrt{3} = \sqrt{3}\,,\\
&\overline{7} \cdot \sqrt{2} = \sqrt{2}\,, && \overline{5} \cdot \sqrt{3} = -\sqrt{3}\,, && \overline{11} \cdot \sqrt{2} = -\sqrt{2}\,, && \overline{11} \cdot \sqrt{3} = -\sqrt{3}\,.
\end{aligned}$$

6.6 (a) We have

$$|\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})| = [\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \deg \Phi_5(X) = \varphi(5) = 4,$$

and $(\mathbb{Z}/5)^\times$ is cyclic generated by the residue class $\overline{2}$. The Galois action is given by

$$\overline{2} \cdot \zeta_5 = \zeta_5^2, \quad \overline{2}^2 \cdot \zeta_5 = \zeta_5^4, \quad \overline{2}^3 \cdot \zeta_5 = \zeta_5^3, \quad \overline{2}^4 \cdot \zeta_5 = \zeta_5.$$

(b) We have $\zeta_5 + \zeta_5^{-1} = 2\cos(2\pi/5)$ and $\Phi_5(\zeta_5) = 0$, so since $\zeta_5^3 = \zeta_5^{-2}$ and $\zeta_5^4 = \zeta_5^{-1}$,

$$(\zeta_5^2 + \zeta_5^{-2}) + (\zeta_5 + \zeta_5^{-1}) + 1 = 0$$

and therefore

$$(\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1 = 0.$$

Hence

$$4\cos^2(2\pi/5) + 2\cos(2\pi/5) - 1 = 0.$$

The quadratic polynomial $4X^2 + 2X - 1 \in \mathbb{Z}[X]$ has discriminant 20 which is not a square in $\mathbb{Q}$, so this polynomial is irreducible over $\mathbb{Q}$, therefore

$$\operatorname{minpoly}_{\mathbb{Q},\cos(2\pi/5)}(X) = X^2 + \frac{1}{2}X - \frac{1}{4}\,.$$

The roots of this are $\dfrac{-1 \pm \sqrt{5}}{4}$. As $\cos(2\pi/5) > 0$ we must have $\cos(2\pi/5) = \dfrac{-1+\sqrt{5}}{4}$. We also have $\cos(4\pi/5) = \dfrac{-1-\sqrt{5}}{4}$. As $\sin(2\pi/5) > 0$,

$$\sin^2(2\pi/5) = 1 - \cos^2(2\pi/5) = 1 - \frac{1+5-2\sqrt{5}}{16} = \frac{5+\sqrt{5}}{8}\,,$$

hence $\sin(2\pi/5) = \sqrt{\dfrac{5+\sqrt{5}}{8}}\,.$

(c) $\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/4$ and has 3 subgroups $\{\overline{1}\} \leqslant \{\overline{1}, \overline{4}\} \leqslant \operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, giving the following tower of subfields.

$$\begin{array}{c}
\mathbb{Q}(\zeta_5)\\
\Big|\,{\scriptstyle 2}\\
\mathbb{Q}(\zeta_5)^{\langle\overline{4}\rangle} = \mathbb{Q}(\cos(2\pi/5)) = \mathbb{Q}(\sqrt{5}\,)\\
\Big|\,{\scriptstyle 2}\\
\mathbb{Q}
\end{array}$$

6.7 (a) We have

$$\begin{aligned}\xi^2 = \prod_{r=1}^{(p-1)/2} (\zeta_p^r - \zeta_p^{-r})^2 &= (-1)^{(p-1)/2} \prod_{r=1}^{(p-1)/2} (\zeta_p^r - \zeta_p^{-r})(\zeta_p^{-r} - \zeta_p^r) \\ &= (-1)^{(p-1)/2} \prod_{r=1}^{(p-1)/2} (1-\zeta_p^{-2r})(1-\zeta_p^{2r}) \\ &= (-1)^{(p-1)/2} \prod_{r=1}^{p-1} (1-\zeta_p^{2r}) \\ &= (-1)^{(p-1)/2} \prod_{s=1}^{(p-1)} (1-\zeta_p^{s})\end{aligned}$$

since each congruence $2x \equiv t \pmod p$ has exactly one solution modulo p for each t.
(b) Since

$$(-1)^{(p-1)/2} = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

and

$$\prod_{s=1}^{p-1} (1-\zeta_p^s) = \Phi_p(1) = p,$$

the result follows.
(c) Taking square roots we find that

$$\xi = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm\sqrt{p}\, i & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

As $\xi \in \mathbb{Q}(\zeta_p)$, we see that $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$ and $\sqrt{p}\, i \in \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$.

6.8 Recall the well-known formula

$$\sigma(i_1 \ \cdots \ i_r)\sigma^{-1} = (\sigma(i_1) \ \cdots \ \sigma(i_r)).$$

Then for $1 \leqslant r \leqslant n-2$ we have

$$(1\ 2\ \cdots\ n)^r (1\ 2)(1\ 2\ \cdots\ n)^{n-r} = (1\ 2\ \cdots\ n)^r (1\ 2)((1\ 2\ \cdots\ n)^r)^{-1} = (r+1\ r+2),$$

while

$$(1\ 2\ \cdots\ n)^{n-1}(1\ 2)((1\ 2\ \cdots\ n)^{n-1})^{-1} = (1\ 2\ \cdots\ n)^{-1}(1\ 2)((1\ 2\ \cdots\ n)^{-1})^{-1} = (n\ 1) = (1\ n).$$

This means that every such 2-cycle $(r+1\ r+2)$ is in H. Also recall that every permutation $\rho \in \mathrm{S}_n$ is a product of 2-cycles, so it suffices to show that every 2-cycle $(a\ b) \in \mathrm{S}_n$ is a product of 2-cycles of the form $(r+1\ r+2)$. Assuming that $a < b$, we also have

$$(a\ b) = (b-1\ b)\cdots(a+2\ a+3)(a+1\ a+2)(a\ a+1)(a+1\ a+2)(a+2\ a+3)\cdots(b-1\ b),$$

and this is in H. Hence $H = \mathrm{S}_n$.

6.9 (a) For each $u \in E$,

$$\begin{aligned}\sigma(T(u)) &= \sigma(u + \sigma(u) + \sigma^2(u) + \cdots + \sigma^{n-1}(u)) \\ &= \sigma(u) + \sigma^2(u) + \cdots + \sigma^n(u) \\ &= \sigma(u) + \sigma^2(u) + \cdots + \sigma^{n-1}(u) + u = T(u),\end{aligned}$$

so $T(u)$ is fixed by σ and all its powers, hence by $\mathrm{Gal}(E/K)$. Therefore $T(u)$ is in $E^{\mathrm{Gal}(E/K)} = K$. It is straightforward to verify that the resulting function $\mathrm{Tr}_{E/K}\colon E \longrightarrow K$ is K-linear.
(b) Let $v \in E$ and suppose that $\mathrm{Tr}_{E/K}(v) = 0$. By Artin's Theorem 6.15, the linear combination of characters $\mathrm{id} + \sigma + \cdots + \sigma^{n-1}$ must be linearly independent, so there is an element $t \in E$ for which

$$\mathrm{Tr}_{E/K}\, t = t + \sigma(t) + \cdots + \sigma^{n-1}(t) \neq 0.$$

Then

$$u = v\sigma(t) + (v + \sigma(v))\sigma^2(t) + \cdots + (v + \sigma(v)\sigma^2(t) + \cdots + \sigma^{n-2}(v))\sigma^{n-1}(t)$$

satisfies

$$\begin{aligned} u - \sigma(u) &= v\left(\sigma(t) + \sigma^2(t) + \cdots + \sigma^{n-1}(t)\right) - \left(\sigma(v) + \cdots + \sigma^{n-1}(v)\right)t \\ &= v\left(t + \sigma(t) + \sigma^2(t) + \cdots + \sigma^{n-1}(t)\right) - \left(v + \sigma(v) + \cdots + \sigma^{n-1}(v)\right)t \\ &= (\mathrm{Tr}_{E/K}\, t)v - (\mathrm{Tr}_{E/K}\, v)t = (\mathrm{Tr}_{E/K}\, t)v. \end{aligned}$$

So we obtain

$$v = \frac{1}{\mathrm{Tr}_{E/K}\, t}\, u - \sigma\left(\frac{1}{\mathrm{Tr}_{E/K}\, t}\, u\right).$$

6.10 (a) This can be proved by induction on n. Write

$$e_r^{[m]} = \sum_{i_1 < i_2 < \cdots < i_r \leqslant m} X_{i_1} \cdots X_{i_r}, \quad s_r^{[m]} = \sum_{1 \leqslant i \leqslant m} X_i^r.$$

Then we easily find that

$$e_r^{[m]} = e_r^{[m-1]} + e_{r-1}^{[m-1]} X_m, \quad s_r^{[m]} = s_r^{[m-1]} + X_m^r.$$

Notice also that $e_r^{[m]} = 0$ whenever $r > m$. The desired result is that for all $n \geqslant 1$ and $k \geqslant 1$,

$$s_k^{[n]} = e_1^{[n]} s_{k-1}^{[n]} - e_2^{[n]} s_{k-2}^{[n]} + \cdots + (-1)^{k-1} e_{k-1}^{[n]} s_1^{[n]} + (-1)^k k e_k^{[n]}.$$

When $n = 1$ we have $s_r^{[1]} = X_1^r$ and $e_1^{[1]} = X_1$ from which the result follows. Now suppose that the result is true for some $n \geqslant 1$. Then $s_k^{[n+1]} = s_k^{[n]} + X_{n+1}^k$, while

$$\begin{aligned} &e_1^{[n+1]} s_{k-1}^{[n+1]} - e_2^{[n+1]} s_{k-2}^{[n+1]} + \cdots + (-1)^{k-1} e_{k-1}^{[n+1]} s_1^{[n+1]} + (-1)^k k e_k^{[n+1]} = \\ &\qquad (e_1^{[n]} + X_{n+1})(s_{k-1}^{[n]} + X_{n+1}^{k-1}) - (e_2^{[n]} + e_1^{[n]} X_{n+1})(s_{k-2}^{[n]} + X_{n+1}^{k-2}) + \cdots \\ &\qquad\qquad + (-1)^{k-1}(e_{k-1}^{[n]} + e_{k-2}^{[n]} X_{n+1})(s_1^{[n]} + X_{n+1}) + (-1)^k k (e_k^{[n]} + e_{k-1}^{[n]} X_{n+1}) \\ &\qquad\qquad = s_k^{[n]} + (e_1^{[n]} X_{n+1}^{k-1} - e_2^{[n]} X_{n+1}^{k-2} + \cdots + (-1)^{k-1} e_{k-1}^{[n]} X_{n+1}) \\ &\qquad\qquad\qquad + (s_{k-1}^{[n]} - e_1^{[n]} s_{k-2}^{[n]} + \cdots + (-1)^{k-1} e_{k-2}^{[n]} s_1^{[n]} + (-1)^k k e_{k-1}^{[n]}) X_{n+1} \\ &\qquad\qquad\qquad\qquad + (X_{n+1}^k - e_1^{[n]} X_{n+1}^{k-1} + \cdots + (-1)^{k-1} e_{k-2}^{[n]} X_{n+1}^2) \\ &\qquad\qquad\qquad\qquad\qquad\qquad = s_k^{[n]} + X_{n+1}^k = s_k^{[n+1]}, \end{aligned}$$

which demonstrates the inductive step.
(b)(i) We have $h_1 = e_1$, $h_2 = e_1^2 - e_2$ and $h_3 = e_3 - 2e_1e_2 + e_1^3$.
(ii) This can be done by induction on n in a similar way to part (a).