Solution 12

Algebraic closure, splitting field

1. Let K be a field of characteristic $\neq 2$ and L/K a field extension of degree 2. Show that there exists $\alpha \in L$ such that $\alpha^2 \in K$ and $L = K(\alpha)$. What is $\mathrm{irr}(\alpha, K)$?

   Solution: First notice that $\mathrm{char}(L) \neq 2$ as well, since otherwise $0 = 2 \cdot 1_L = 2 \cdot 1_K$, contradiction. Hence $\frac{1}{2} \in K \subseteq L$. Since $[L : K] = 2$, the extension is not trivial and there exists $\beta \in L \setminus K$. Then $[L : K(\beta)][K(\beta) : K] = [L : K] = 2$ forces $L = K(\beta)$ and in particular $\deg(\mathrm{irr}(\beta, K)) = [K(\beta) : K] = 2$. Write $\mathrm{irr}(\beta, K) = X^2 + aX + b$. Then

   $$0 = \beta^2 + a\beta + b = \left(\beta + \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right),$$

   so that for $\alpha = \beta + \frac{a}{2}$ we see that $\alpha^2 = \frac{a^2}{4} - b \in K$ and that $K(\alpha) = K(\beta) = L$.

2. Let $L = K(\alpha)/K$ be a field extension such that $[L : K]$ is odd. Prove that $L = K(\alpha^2)$.

   Solution: Clearly, $K(\alpha^2) \subset K(\alpha) = L$. Notice that the element $\alpha \in L$ is a root of $X^2 - \alpha^2 \in K(\alpha^2)[X]$. This implies that $[L : K(\alpha^2)] = \deg(\mathrm{irr}(\alpha, K)) \leqslant 2$. On the other hand, $[L : K(\alpha^2)][K(\alpha^2) : K] = [L : K]$ is odd, so that $[L : K(\alpha^2)]$ must be odd, too. Hence $[L : K(\alpha^2)] = 1$, meaning that $L = K(\alpha^2)$.

3. Let $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{C}$

   (a) Show that α is algebraic over $\mathbb{Q}$.

   (b) Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. [*Hint:* $\alpha + \alpha^{-1} \in \mathbb{Q}(\alpha)$]

   (c) Determine $\mathrm{irr}(\alpha, \mathbb{Q})$.

   Solution:

   (a) Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $\sqrt{3}$ is a root of $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$, so that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leqslant 2$, the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is finite and hence algebraic. In particular, $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is algebraic over $\mathbb{Q}$.

   (b) Since $\mathbb{Q}(\alpha) \ni \alpha + \alpha^{-1} = \sqrt{2} + \sqrt{3} - \sqrt{2} + \sqrt{3} = 2\sqrt{3}$, we know that $\sqrt{3} \in \mathbb{Q}(\alpha)$ and $\sqrt{2} = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha)$. This implies that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Notice that $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ is irreducible, because otherwise it would have a root in $\mathbb{Q}(\sqrt{2})$, which is not the case [indeed, writing a general element of $\mathbb{Q}(\sqrt{2})$ as

$s + t\sqrt{2}$ for $s, t \in \mathbb{Q}$, we see that $3 = (s + t\sqrt{2})^2 = s^2 + 2t^2 + 2st\sqrt{2}$ implies that $st = 0$, so that $3 = s^2$ or $3 = 2t^2$, which are impossible equalities]. Hence $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and we can conclude that

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

(c) Squaring both sides of $\sqrt{3} = \alpha - \sqrt{2}$ we obtain $3 = \alpha^2 - 2\sqrt{2} + 2$, that is, $2\sqrt{2} = \alpha^2 - 1$. Squaring this equality, we get $8 = \alpha^4 - 2\alpha^2 + 1$. Hence α is a root of the polynomial $f := X^4 - 10X^2 + 1$, so that $\mathrm{irr}(\alpha, \mathbb{Q}) | f$. But $\deg(\mathrm{irr}(\alpha, \mathbb{Q})) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = \deg(f)$, so that

$$\mathrm{irr}(\alpha, \mathbb{Q}) = f = X^4 - 10X^2 + 1.$$

4. Let p be a prime number. For $d \geqslant 1$, let N_d be the number of monic irreducible polynomials in $\mathbb{F}_p[X]$ of degree d.

(a) Compute N_1 and N_2.

(b) Let $n \in \mathbb{Z}_{>1}$. Using the description of finite fields stated in class, prove that $X^{p^n} - X$ is the product of all irreducible monic polynomials over $\mathbb{F}_p$ whose degree divides n.

(c) Deduce that

$$\sum_{d|n} dN_d = p^n,$$

where d runs over divisors $d \geqslant 1$ of n.

(d) Prove that

$$\lim_{n \longrightarrow \infty} \frac{N_n}{(p^n/n)} = 1.$$

[*Hint:* $p^n - \sum_{d|n, d<n} dN_d = nN_n \leqslant p^n$. Notice that $N_d \leqslant p^d$ and $d \leqslant n/2$ for $d < n$. Use this to estimate $\frac{1}{n} \sum_{d|n, d<n} dN_d$ and conclude]

Solution:

(a) A monic polynomial of degree 1 in $\mathbb{F}_p$ can be written as $X + a$ for $a \in \mathbb{F}_p$. This is an irreducible polynomial for each $a \in \mathbb{F}_p$, so that

$$N_1 = p.$$

In degree 2, we see that there are p^2 monic polynomials (corresponding to the choices of coefficients a_1, a_2 in the expression $X^2 + a_1X + a_2$). Among those, there are the non-irreducible polynomials, which can all written as $(X - b_1)(X - b_2)$ in a unique way up to switching b_1 and b_2, so that there are $p + \binom{p}{2} = \frac{p^2+p}{2}$ non-irreducible monic polynomials of degree 2. Hence

$$N_2 = p^2 - \frac{p^2 + p}{2} = \frac{p^2 - p}{2}.$$

(b) Fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. As seen in class, for each $m \in \mathbb{Z}_{>1}$ there exists a unique subfield of $\overline{\mathbb{F}_p}$ containing p^m elements, that is,

$$\mathbb{F}_{p^m} = \{y \in \overline{\mathbb{F}_p} : y^{p^m} = y\}.$$

In particular, $\mathbb{F}_{p^n}$ is the set of roots of $X^{p^n} - X$ and since its cardinality is equal to the degree of the polynomial and the polynomials $X - \alpha \in \mathbb{F}_{p^n}$ are coprime, we know that

$$X^{p^n} - X = \prod_{\alpha \in \mathbb{F}_{p^n}} (X - \alpha).$$

For every $\alpha \in \mathbb{F}_{p^n}$ we know that $\deg(\mathrm{irr}(\alpha, \mathbb{F}_p)) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] | [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so that $X - \alpha$ divides the product of all monic irreducible polynomials whose degree divides n. As the polynomials $X - \alpha$ are pairwise coprime in $\mathbb{F}_{p^n}$, we obtain that

$$X^{p^n} - X = \prod_{\alpha \in \mathbb{F}_{p^n}} (X - \alpha) \,|\, \prod_{\substack{f \in \mathbb{F}_p[X] \text{ irr. monic} \\ \deg(f) | n}} f.$$

Conversely, let $f \in \mathbb{F}_p[X]$ be a monic irreducible polynomial of degree $d|n$. Let $x \in \overline{\mathbb{F}_p}$ be a root of f, so that $f = \mathrm{irr}(x, \mathbb{F}_p)$ and $[\mathbb{F}_p(x) : \mathbb{F}_p] = d$, which implies that $\mathrm{Card}(\mathbb{F}_p(x)) = p^d$. Hence $\mathbb{F}_p(x) = \mathbb{F}_{p^d}$ and in particular $x^{p^d} = x$. Write $n = d\ell$ for $\ell \in \mathbb{N}$. Since $p^n = (p^d)^\ell$, we see that x^{p^n} is obtained by repeatedly raising x to the p^d-th power for ℓ times, so that $x^{p^n} = x$. Hence x is a root of $X^{p^n} - X$, which implies that $f = \mathrm{irr}(x, \mathbb{F}_p)$ divides $X^{p^n} - X$. By arbitrarity of f and since two distinct irreducible monic polynomials in $\mathbb{F}_p[X]$ must be coprime, we obtain that

$$\prod_{\substack{f \in \mathbb{F}_p[X] \text{ irr. monic} \\ \deg(f) | n}} f \,|\, X^{p^n} - X.$$

Since the two polynomials are associated in $\mathbb{F}_p[X]$ and both monic, they must coincide.

(c) This follows immediately from part (b), by comparing the degrees. Indeed,

$$\begin{aligned} p^n = \deg(X^{p^n} - X) = \deg\left(\prod_{\substack{f \in \mathbb{F}_p[X] \text{ irr. monic} \\ \deg(f) | n}} f \right) &= \sum_{d|n} \Big(\sum_{\substack{f \in \mathbb{F}_p[X] \text{ irr. monic} \\ \deg(f) = d}} \deg(f) \Big) \\ &= \sum_{d|n} d N_d. \end{aligned}$$

(d) The number of monic polynomials in $\mathbb{F}_p$ of degree d is p^d, so that $N_d \leqslant p^d$ for all d. If d is a proper divisor of n, then $d\ell = n$ for $\ell \geqslant 2$, so that $d \leqslant n/2$. In particular, the number of proper divisors of n is less than $n/2$. Hence

$$\frac{1}{n}\sum_{d|n,d<n} dN_d \leqslant \frac{1}{n}\frac{n}{2}\cdot\frac{n}{2}\cdot p^n = \frac{n}{4}p^{\frac{n}{2}}. \tag{1}$$

By the initial observation and by part (c), we know that $p^n - \sum_{d|n,d<n} dN_d = nN_n \leqslant p^n$, which divided by p^n gives

$$1 - \frac{n}{p^n}\frac{1}{n}\sum_{d|n,d<n} dN_d = \frac{N_n}{p^n/n} \leqslant 1$$

By (1), we notice that

$$0 \leqslant \frac{n}{p^n}\frac{1}{n}\sum_{d|n,d<n} dN_d \leqslant \frac{n}{p^n}\frac{n}{4}p^{\frac{n}{2}} = \frac{n^2}{4p^{\frac{n}{2}}} \xrightarrow{n\to\infty} 0$$

and we can conclude that $\frac{N_n}{p^n/n} \longrightarrow 1$ for $n \longrightarrow \infty$.

5. Prove that $\overline{\mathbb{Q}} \subset \mathbb{C}$ is countable.

Solution: First notice that $\overline{\mathbb{Q}}$ is infinite because it contains $\mathbb{N}$.

If α is an algebraic number, there exists a unique irreducible polynomial $f_\alpha \in \mathbb{Z}[X]$ (in particular, f is primitive) with positive leading coefficient—it is obtained by multiplying $\operatorname{irr}(\alpha, \mathbb{Q})$ by the greatest common divisor of its coefficients. Thus for each $\alpha \in \overline{\mathbb{Q}}$ there exist unique $n_\alpha \in \mathbb{N}$ and $a_0^\alpha, \dots, a_{n_\alpha}^\alpha \in \mathbb{Z}_{>0}$ such that $a_{n_\alpha}^\alpha > 0$ and

$$f_\alpha = a_{n_\alpha}^\alpha X^{n_\alpha} + \ldots + a_1^\alpha X + a_0^\alpha.$$

Define, for $N \in \mathbb{N}$,

$$X_N := \{\alpha \in \overline{\mathbb{Q}} : n_\alpha \leqslant N,\, \forall i = 1, \dots, n_\alpha\, |a_i| \leqslant N\}.$$

By construction,

$$\bigcup_{N\in\mathbb{N}} X_N = \overline{\mathbb{Q}}.$$

Moreover, each X_N has a finite cardinality. Indeed, for a fixed N, there are $N+1$ possible values of n_α, for each of which there are no more than $(2N+1)^{n_\alpha}$ values for the coefficients a_i and for each of the finitely many admissible tuples $(n_\alpha, a_0^\alpha, \dots, a_{n_\alpha}^\alpha)$ which actually gives an irreducible polynomial there are at most n_α roots that can be chosen as initial $\alpha \in \overline{\mathbb{Q}}$. This implies that $\overline{\mathbb{Q}}$ is a countable union of finite sets and as such it is countable.

6. Let K be a field and $f \in K[X]$ a non-constant polynomial. Let L be a splitting field of f. Show that $[L : K] \leqslant \deg(f)!$.

   Solution: We recall the procedure used to prove existence of the splitting field. Let g be an irreducible factor of f. Then K can be seen as a subfield of $K_1 := K[X]/(g) \ni [X] =: \alpha$. In L_1, the image of f is divisible by $X - \alpha$. By uniqueness of the splitting field, the splitting field L of f over K is isomorphic as a K-extension to the splitting field L' of $h = \frac{f}{X-\alpha}$ over K'. Since $\deg(h) = \deg(f) - 1$, we can work by induction on $\deg(f)$, and get

$$\begin{aligned}[L : K] &= [L' : K] = [L' : K_1][K_1 : K] \\ &= \deg(g)[L' : K_1] \leqslant \deg(f)[L : K_1] \leqslant \deg(f)(\deg(f) - 1)! = \deg(f)!\end{aligned}$$

   where in the last inequality we supposed that our result works for degree $\deg(f)-1$.

7. (Trace and norm for finite field extensions) Let L/K be a finite field extension.

   (a) For $x \in L$, show that the following is a K-linear map:

$$\begin{aligned} m_x : L &\longrightarrow L \\ y &\longmapsto xy \end{aligned}$$

   (b) Show that the map $r_{L/K} : L \longrightarrow \mathrm{End}_K(L)$ sending $x \mapsto m_x$ is a ring homomorphism.

   (c) Consider the maps

$$\begin{aligned} \mathrm{Tr}_{L/K} : L &\longrightarrow K && \text{(trace map)} \\ x &\longmapsto \mathrm{Tr}(m_x), \\ \mathrm{N}_{L/K} : L &\longrightarrow K && \text{(norm map)} \\ x &\longmapsto \det(m_x). \end{aligned}$$

   Prove:

   - $\mathrm{Tr}_{L/K}$ is K-linear.
   - $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$ for all $x, y \in L$ and $\mathrm{N}_{L/K}(x) = 0$ if and only if $x = 0$.

   (d) Given a tower of finite extensions $L_1/L_2/K$, show that

$$\mathrm{Tr}_{L_1/K} = \mathrm{Tr}_{L_2/K} \circ \mathrm{Tr}_{L_1/L_2}.$$

   [*Hint:* Write down a K-basis of L_1 starting from a K-basis of L_2 and an L_2-basis of L_1, then evaluate the right-hand side on $\alpha \in L_1$].

   (e) Prove that if $x \in L$ is such that $L = K(x)$, and

$$\mathrm{irr}(x, K)(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in K[X],$$

   then $\mathrm{Tr}_{L/K}(x) = -a_{d-1}$ and $\mathrm{N}_{L/K}(x) = (-1)^d a_0$. [*Hint:* $(1, x, \ldots, x^{d-1})$ is a K-basis of L.]

(f) Let p be an odd prime number, $\zeta = e^{\frac{2\pi i}{p}}$ and $K = \mathbb{Q}(\zeta)$ (see Assignment 11, Exercise 4). Compute: $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta)$, $\mathrm{N}_{K/\mathbb{Q}}(\zeta)$ and $\mathrm{N}_{K/\mathbb{Q}}(\zeta - 1)$.

Solution:

(a) It is immediate to check K-linearity of each map m_x. Indeed, m_x is additive by distributivity of the multiplication with respect to addition, and it respect scalar multiplication by commutativity of the multiplication in L.

(b) We immediately notice that $m_0 = 0$ and $m_1 = \mathrm{id}_L$. For $x, y, z \in L$, we have $m_{x+y}(z) = (x+y)z = xz + yz = m_x(z) + m_y(z)$ and $m_{xy}(z) = (xy)z = x(yz) = m_x(m_y(z)) = (m_x \circ m_y)(z)$. This means that $r_{L/K}$ respects both sum and multiplication, and we can conclude that it is a ring homomorphism. As $r_{L/K}$ is not the zero map (since it sends $1 \mapsto id_L \neq 0$) and L is a field, the kernel is equal to (0), so that $r_{L/K}$ is injective.

(c) First, we prove linearity of $\mathrm{Tr}_{L/K}$. Let $n = [L : K]$ and fix a K-basis $\mathcal{B}$ for L. Then by basic linear algebra we have a K-linear ring isomorphism $\varphi : \mathrm{End}_K(L) \longrightarrow M_n(K)$. Also, the trace map $\mathrm{tr} : M_n(K) \longrightarrow K$ is easily seen to be K-linear. Then by construction we have that $\mathrm{Tr}_{L/K} = \mathrm{tr} \circ \varphi \circ r_{L/K}$, which is K-linear as it is a composition of K-linear maps.

As concerns norm, we have $\mathrm{N}_{L/K} = \det \circ \varphi \circ r_{L/K}$. Since all the composed maps respect multiplication, so does $\mathrm{N}_{L/K}$. Moreover, we have $\mathrm{N}_{L/K}(x) = 0$ if and only if $\det(m_x) = 0$, which is equivalent to saying that m_x is not an invertible endomorphism, and this happens precisely when $x = 0$ (since for $x \neq 0$, me have $m_{x^{-1}} = m_x^{-1}$).

(d) Let $\mathcal{B}_1 = (e_1, \ldots, e_k)$ be an L_2-basis for L_1, and $\mathcal{B}_2 = (f_1, \ldots, f_l)$ be an K-basis for L_2. As seen in class,

$$\mathcal{B} := (e_1 f_1, e_1 f_2, \ldots, e_1 f_l, e_2 f_1, \ldots, e_2 f_l, \ldots, e_k f_1, \ldots, e_k f_l)$$

is a K-basis for L_1.

For $\alpha \in L_1$, we can find coefficients $\lambda_{ij} \in L_2$, with $1 \leqslant i, j \leqslant k$, so that for each i one has

$$\alpha \cdot e_i = \sum_{j=1}^{k} \lambda_{ij} e_j.$$

Then for each i, j as above and $1 \leqslant s, t \leqslant l$ we can find coefficients $\mu_{ijst} \in L_2$ such that for each i, j and s one has

$$\lambda_{ij} \cdot f_s = \sum_{t=1}^{l} \mu_{ijst} f_t.$$

Putting those two equalities together we get, for each i and t as above,

$$\alpha \cdot e_i f_s = \sum_{j=1}^{k} \sum_{t=1}^{l} \mu_{ijst} e_j f_t$$

Then the matrix correspondent to m_α as a L_2-linear map of L_1, with respect to the basis $\mathcal{B}_1$, is

$$[m_\alpha]_{L_1/L_2} = {}^T(\lambda_{ij})_{i,j},$$

so that $\mathrm{Tr}_{L_1/L_2}(\alpha) = \sum_{i=1}^k \lambda_{ii}$. Moreover, the matrix correspondent to m_α as a K-linear map of L_1, with respect to the basis $\mathcal{B}$, is

$$[m_\alpha]_{L_1/K} = {}^T(\mu_{ijst})_{(i,s),(j,t)},$$

where the row index is the couple (i,s) and the column index is the couple (j,t), and row (column) indexes are ordered with lexicographical order, so that $\mathrm{Tr}_{L_1/K}(\alpha) = \sum_{i=1}^k \sum_{s=1}^l \mu_{iiss}$.
Furthermore, for each i,j as before, the matrix correspondent to $m_{\lambda_{i,j}}$ as a K-linear map of L_2, with respect to the basis $\mathcal{B}_2$, is

$$[m_{\lambda_{i,j}}]_{L_2/K} = {}^T(\mu_{ijst})_{s,t},$$

so that $\mathrm{Tr}_{L_2/K}(\lambda_{ij}) = \sum_{s=1}^l \mu_{ijss}$.
In conclusion, we have

$$\begin{aligned}\mathrm{Tr}_{L_2/K}(\mathrm{Tr}_{L_1/L_2}(\alpha)) = \mathrm{Tr}_{L_2/K}(\sum_{i=1}^k \lambda_{ii}) &= \sum_{i=1}^k \mathrm{Tr}_{L_2/K}(\lambda_{ii}) \\ &= \sum_{i=1}^k \sum_{s=1}^l \mu_{iiss} = \mathrm{Tr}_{L_1/K}(\alpha).\end{aligned}$$

(e) Since $L \cong K[X]/(\mathrm{irr}(x,\mathbb{Q}))$ as field extensions of K and $(1, x, \dots, x^{d-1})$ is a K-basis of L, we are interested in the matrix $M_x = (\lambda_{ij})_{0\leqslant i,j\leqslant d-1}$ associated to m_x. For $j = 0, \dots, d-2$, we have $x \cdot x^j = x^{j+1}$ so that we have

$$\lambda_{ij} = \begin{cases} 1 & \text{if } i = j+1 \\ 0 & \text{else.} \end{cases}, \text{ for } j = 0, \dots, d-2.$$

Moreover, $x \cdot x^{d-1} = x^d = -a_0 - a_1 x - \dots - a_{d-1}x^{d-1}$, so that

$$\lambda_{i,(d-1)} = -a_i.$$

What we have found is

$$M_x = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Then we get $\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(M_x) = -a_{d-1}$, and using Legendre form for the determinant on the first row we also obtain $\mathrm{N}_{L/K}(x) = \det(M_x) = (-1)^d a_0$.

(f) By Assignment 11, Exercise 4, the minimal polynomial of ζ is

$$\Phi_p := \frac{X^p - 1}{X - 1}.$$

By part (e), $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta) = -1$ and $\mathrm{N}_{K/\mathbb{Q}}(\zeta) = 1$, since p is odd. Notice that $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta - 1)$, so that $\mathrm{Irr}(\zeta - 1, \mathbb{Q})$ has degree $p - 1$. Since $\zeta - 1$ satisfies $G(X) := \varphi(X + 1)$ which is irreducible of degree $p - 1$, we get

$$\mathrm{Irr}(\zeta - 1, \mathbb{Q}) = \frac{(X + 1)^p - 1}{X},$$

whose constant coefficient has been seen in Assignment 11, Exercise 4 to be equal to p. Then $N_{L/K}(\zeta - 1) = p$.