Solution 13

Finite Fields, Modules over a commutative ring

1. Let L be a fixed algebraic closure of $\mathbb{F}_p$ and, for each $n \in \mathbb{Z}_{>0}$, let $\mathbb{F}_{p^n} \subseteq L$ the unique subfield of cardinality p^n.

   (a) Show that $L = \bigcup_{n \geqslant 1} \mathbb{F}_{p^n}$.

   (b) Show that $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ if and only if $n|m$.

   (c) Let $x \in \mathbb{F}_{p^n}$ for some $n \geqslant 1$. Prove that
   $$x + x^p + \ldots + x^{p^{n-1}} \in \mathbb{F}_p$$
   and
   $$x^{1+p+\cdots+p^{n-1}} \in \mathbb{F}_p.$$

   (d) Define the norm map $N : \mathbb{F}_{p^n}^\times \longrightarrow \mathbb{F}_p^\times$ by sending $x \mapsto x^{1+p+\cdots+p^{n-1}}$. Prove that it is a surjective group homomorphism. [*Hint:* For surjectivity, take a generator x of $\mathbb{F}_{p^n}^\times$ and find the order of $N(x)$]

   Solution:

   (a) Each $\mathbb{F}_{p^n}$ lies in L by definition, so that $\bigcup_{n\geqslant 1} \mathbb{F}_{p^n} \subset L$. Conversely, for every $\alpha \in L$, the extension $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is finite of degree $d := \deg(\mathrm{irr}(\alpha, \mathbb{F}_p))$. Hence $\mathbb{F}_p(\alpha)$ is a subfield of cardinality p^d which means that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$, implying that $\alpha \in \bigcup_{n\geqslant 1} \mathbb{F}_{p^n}$. As we have proven both inclusions, we can conclude that $L = \bigcup_{n\geqslant 1} \mathbb{F}_{p^n}$.

   (b) Recall the characterization of $\mathbb{F}_{p^n}$ in terms of the Frobenius isomorphism $\mathrm{Fr} : L \longrightarrow L$ (sending $x \mapsto x^p$):
   $$\mathbb{F}_{p^n} = \{\alpha \in \mathbb{F}_{p^n} : \mathrm{Fr}^n(\alpha) = \alpha\}.$$
   If $n|m$, say $m = nk$, then $\mathrm{Fr}^m = (\mathrm{Fr}^n)^k$, so that by the above characterization $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$.
   Conversely assume that $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ and write $m = kn + r$ for $0 \leqslant r < n$. Then $\mathrm{Fr}^m(\alpha) = \mathrm{Fr}^n(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$, which means that
   $$\alpha = \mathrm{Fr}^m(\alpha) = \mathrm{Fr}^r((\mathrm{Fr}^n)^k(\alpha)) = \mathrm{Fr}^r(\alpha).$$
   For $r \neq 0$, this implies that $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^r}$, a contradiction. Hence $r = 0$ and $n|m$.

(c) If $x \in \mathbb{F}_{p^n}$, then $x = \mathrm{Fr}^n(x) = x^{p^n}$. In particular,

$$\mathrm{Fr}(x + x^p + \ldots + x^{p^{n-1}}) = x^p + x^{p^2} + \ldots + x^{p^n} = x + x^p + x^{p^2} + \ldots + x^{p^n-1},$$
$$\mathrm{Fr}(x^{1+p+\cdots+p^{n-1}}) = x^{p(1+p+\cdots+p^{n-1})} = x^{p+p^2+\cdots+p^n} = x^{1+p+p^2\cdots+p^{n-1}},$$

so that $x + x^p + \ldots + x^{p^{n-1}}$ and $x^{1+p+p^2\cdots+p^{n-1}}$ are fixed by Fr, which implies that they lie in $\mathbb{F}_p$.

(d) By part (c), $x \mapsto x^{1+p+\cdots+p^{n-1}}$ defines a map $\mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$. Since $\mathbb{F}_{p^n}$ is a field, $x^{1+p+\cdots+p^{n-1}} = 0$ if and only if $x = 0$, so that $N : \mathbb{F}_{p^n}^\times \longrightarrow \mathbb{F}_p^\times$ is a well-defined map. It is a group homomorphism because $\mathbb{F}_{p^n}^\times$ is an abelian group, meaning that $(xy)^k = x^k y^k$ for each $x, y \in \mathbb{F}_{p^n}^\times$ and $k \in \mathbb{Z}$.
Let x be a generator of $\mathbb{F}_{p^n}^\times$. Then x has order $p^n - 1$. Since

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

the element $N(x) = x^{1+p+\cdots+p^{n-1}} \in \mathbb{F}_{p^n}^\times$ has order $p - 1$, so that it is a generator of $\mathbb{F}_p^\times$, implying that N is surjective.

2. Let $\mathbb{F}_q$ be a finite field of cardinality $q = p^n$ and $f \in K[X]$ an irreducible polynomial of degree $d \geqslant 1$.

(a) Prove that f divides the polynomial $X^{q^m} - X$ if and only if $d|m$.

(b) Let x be a root of f in a fixed algebraic closure $\overline{\mathbb{F}_q}$. Show that the roots of f are

$$x,\ x^q,\ \ldots, x^{q^{d-1}}.$$

(c) Assume that $p \neq 2$ and let $\varepsilon \in \mathbb{F}_q^\times$ be such that ε is not a square in $\mathbb{F}_q$. Let $\alpha \in \overline{\mathbb{F}_q}$ be such that $\alpha^2 = \varepsilon$ and set $L = \mathbb{F}_q(\alpha)$. For $y = x_0 + \alpha x_1 \in L$, compute y^q.

(d) Prove that the norm map $N : \mathbb{F}_{p^n}^\times \longrightarrow \mathbb{F}_p^\times$ defined in Exercise 1(d) coincides with the one defined in Assignment 12, Exercise 7.

Solution:

(a) Fix an algebraic closure $\overline{\mathbb{F}_q} = \overline{\mathbb{F}_p}$ of $\mathbb{F}_q$. Let $\alpha \in \overline{\mathbb{F}_q}$ be a root of f, so that $f = \lambda\, \mathrm{irr}(\alpha, \mathbb{Q})$ for some $\lambda \in \mathbb{F}_q^\times$. Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$, so that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d} = \mathbb{F}_{p^{nd}}$, the unique subfield of $\overline{\mathbb{F}_q}$ with q^n elements.
If $d|m$, then, by Exercise 1(b),

$$\alpha \in \mathbb{F}_{q^d} = \mathbb{F}_{p^{nd}} \subset \mathbb{F}_{p^{nm}} = \mathbb{F}_{q^m},$$

so that α is a root of $X^{q^m} - X$ and $\mathrm{irr}(\alpha, \mathbb{Q})|X^{q^m} - X$ by definition of minimal polynomial, which implies that $f|X^{q^m} - X$.
Conversely, if $f|X^{q^m} - X$, then α is a root of $X^{q^m} - X$, so that $\alpha \in \mathbb{F}_{q^m}$. Then $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^m}$, which by Exercise 1(b) implies that $d|m$.

(b) For each $\ell \in \{0, \dots, d-1\}$, we see that

$$0 = (f(x))^{q^\ell} = f(x^{q^\ell}),$$

where the second equality is due to the fact that $a \mapsto a^{q^\ell}$ is the ℓ-th power of the field automorphism Fr^q of $\overline{\mathbb{F}_q}$ sending $a \mapsto a^q$, which respects sums and multiplication and is the identity on $\mathbb{F}_q$ (hence on the coefficients of f). This means that the elements x^{q^ℓ} are all root of f. We claim that those elements are all distinct for $d \in \{0, \dots, d-1\}$. Then they are d distinct roots of f which implies that there are no other roots, because $\deg(f) = d$.

In order to prove our claim, suppose by contradiction that $x^{q^j} = x^{q^k}$ for $0 \leqslant j < k \leqslant d-1$ and let $r = k - j$. Then, raising both sides to the q^{d-k}-th power and recalling that $x^{q^d} = x$ since $\mathbb{F}_q(x) = \mathbb{F}_{q^d}$, we obtain

$$x^{q^{d-(k-j)}} = x,$$

so that $f = \lambda \,\mathrm{irr}(\alpha, \mathbb{F}) \mid X^{q^{d-(k-j)}} - X$, for some $\lambda \in \mathbb{F}_q^\times$, which by part (a) implies that $d | d - (k-j)$, a contradiction.

(c) Let $x_0, x_1 \in \mathbb{F}_q$ and $y = x_0 + \alpha x_1$. If $x_1 = 0$, then $y \in \mathbb{F}_q$, so that $y^q = y = x_0$. Now suppose that $x_1 \neq 0$. Clearly, $[L : \mathbb{F}_q] = \deg(\mathrm{irr}(\alpha, \mathbb{F}_q)) = 2$, because α is a root of $X^2 - \varepsilon$ and $\alpha \notin \mathbb{F}_q$ since ε is not a square in $\mathbb{F}_q$. We notice that

$$\mathbb{F}_q(y) = \mathbb{F}_q(x_0 + \alpha x_1) = \mathbb{F}_q(\alpha) = L,$$

By part (b), y^q is the other root of $\mathrm{irr}(y, \mathbb{Q}) = (X - x_0)^2 - \varepsilon x_1^2$, hence

$$y^q = x_0 - \varepsilon x_1.$$

(d) In this last part, $q = p$. Let x be a generator of $\mathbb{F}_{p^n}^\times$. Since the norm map N is a group homomorphism, it is uniquely determined by $N(x)$. The norm map N_1 defined in Exercise 1(d) is determined by

$$N_1(x) = \prod_{j=0}^{n-1} x^{p^j}. \tag{1}$$

Let $f = \mathrm{irr}(x, \mathbb{F}_p)$. Since $\mathbb{F}_p(x) = \mathbb{F}_{p^n}$ (because $< x >= \mathbb{F}_{p^n}^\times$), we know that $\deg(f) = n$. Write $f = \sum_{k=0}^n a_k X^k$ with $a_n = 1$. The norm map N_2 defined in Assignment 12, Exercise 7, is determined by $N_2(x) = (-1)^n a_0$, because of part (e) of that exercise. But, by part (b), f has n distinct roots $x, x^p, \dots, x^{p^{n-1}}$, so that

$$f = \prod_{j=0}^{n-1} (X - x^{p^j})$$

and $a_0 = (-1)^n \prod_{j=0}^{n-1} x^{p^j}$. Hence

$$N_2(x) = (-1)^n a_0 = \prod_{j=0}^{n-1} x^{p^j} = N_1(x)$$

and the two norms coincide on the generator x and hence on the whole $\mathbb{F}_{p^n}^\times$.

3. (a) Show that 2 is not a square in $\mathbb{F}_{13}$ and let ε be a square root of 2 in $\mathbb{F}_{13^2}$.
   (b) Find all non-squares in $\mathbb{F}_{13}$.
   (c) Express the square roots of all non squares in $\mathbb{F}_{13}$ as elements of $\mathbb{F}_{13^2}$ using the $\mathbb{F}_{13}$-basis $(1, \varepsilon)$.

   Solution:

   (a) Let $S := \{x^2 : x \in \mathbb{F}_{13}^\times\}$ be the set of squares in $\mathbb{F}_{13}^\times$. It is the image of the group automorphism φ of $\mathbb{F}_{13}^\times$ sending $x \mapsto x^2$. Since $\ker(\varphi) = \{1, 12 = -1\}$ (as there are at most two roots of the polynomial $X^2 - 1$), we know that $|S| = 12/2 = 6$ by the First Isomorphism of groups.
   Since $(-x)^2 = x^2$, we see that indeed $S = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\}$, which can be easily computed as

   $$S = \{1, 4, 9, 3, 12, 10\} = \{\pm 1, \pm 3, \pm 4\}.$$

   In particular, 2 is not a square in $\mathbb{F}_{13}$.

   (b) Let $T = \mathbb{F}_{13}^\times \setminus S$ be the set of non-squares. Then, by part (a),

   $$T = \{\pm 2, \pm 5, \pm 6\}.$$

   (c) Since T is the coset of the index-2 subgroup S in $\mathbb{F}_{13}^\times$, the inverse of $t \in T$ is in T, while the product of two elements in T is in S. This means that for any elements $t \in T$ we have $t \cdot (2)^{-1} \in S$, so that we can write the square root of t has a multiple of ε. More precisely:
   - $(-2)/2 = -1 = 5^2$ implies that $-2 = (\pm 5\varepsilon)^2$;
   - $6/2 = 3 = 4^2$ gives $6 = (\pm 4\varepsilon)^2$. Moreover, $-6 = (5^2) \cdot 6$ gives $-6 = (\pm 20\varepsilon)^2 = (\pm 6\varepsilon)^2$;
   - Finally, $5/2 = 9 = 3^2$ gives $5 = (\pm 3\varepsilon)^2$ and $-5 = (\pm 15 \cdot \varepsilon)^2 = (\pm 2 \cdot \varepsilon)^2$.

4. Let R be a commutative ring and $n \geqslant 1$.

   (a) Construct an isomorphism of R-modules

   $$\mathrm{Hom}_{(R\text{-Mod})}(R^n, R^n) \cong R^{n^2}.$$

(b) For $A = (a_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}} \in R^{n^2}$, define

$$\det(A) = \sum_{\sigma\in S_n} \varepsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Prove that, for each $A, B \in R^{n^2}$, $\det(AB) = \det(A)\det(B)$. Prove moreover that $\det(A) \in R^\times$ if and only if A is invertible. [Here, the matrix product is defined with the same formulas as for the usual matrix product over fields]

Solution:

(a) For $j = 1, \dots, n$, consider the element $e_j = (\delta_{ij})_{1\leqslant i\leqslant n} \in R^n$, where $\delta_{ij} = 1_R$ if $i = j$ and $\delta_{ij} = 0_R$ otherwise. The elements e_j form a free R-basis of R^n, so that a morphism $f \in \mathrm{Hom}_{(R\text{-Mod}}(R^n, R^n)$ is uniquely determined by the images $f(e_j)$. Those can be written uniquely as linear combinations

$$f(e_j) = \sum_{i=1}^n a_{ij} e_i.$$

In this way, we have defined a bijection

$$\begin{aligned} \varphi : \mathrm{Hom}_{(R\text{-Mod}}(R^n, R^n) &\longrightarrow R^{n^2} \\ f &\longmapsto (a_{ij})_{ij},\ a_{ij} = \pi_i(f(e_j)), \end{aligned}$$

Since for each $f, g \in \mathrm{Hom}_{(R\text{-Mod}}(R^n, R^n)$ and $r \in R$ we have equalities

$$\pi_i((f + rg)(e_j)) = \pi_i(f(e_j) + r(g(e_j))) = \pi_i(f(e_j)) + r\pi_i(g(e_j)$$

for all i and j, we know that φ is also an isomorphism of R-modules.

(b) Let $M = R^n$ and define $M^n \cong R^{n^2}$ by looking at the n vectors as columns of a matrix. We say that a map $\varphi : M^n \longrightarrow R$ is a *multilinear form* if for each $j = 1, \dots, n$, $r_j \in R$ and $A_1, \dots, A_n, A'_j \in M$ one gets

$$\varphi(A_1, \dots, rA_j + A'_j, \dots, A_n) = r_j\varphi(A_1, \dots, A_n) + \varphi(A_1, \dots, A'_j, \dots, A_n).$$

We say that φ is *alternating* if for every $\varphi(A_1, \dots, A_n) = 0$ when $A_i = A_j$ for $i \neq j$.

If $\varphi : M^n \longrightarrow R$ is a multilinear alternating form then the following property holds:

$$(*)\ \text{For each } \sigma \in S_n,\ \varphi(A_{\sigma(1)}, \dots, A_{\sigma(n)}) = \varepsilon(\sigma)\varphi(A_1, \dots, A_n).$$

Since S_n is generated by transpositions, it is enough to prove (*) for a transposition. For simplicity, we just prove it for $\sigma = (1\,2)$, the proof for other transpositions being analogous. Since φ is linear we have that:

$$\begin{aligned} &\varphi(A_1 + A_2, A_1 + A_2, A_3, \dots, A_n) = \varphi(A_1, A_1, A_3, \dots, A_n) \\ &\quad + \varphi(A_1, A_2, A_3, \dots, A_n) + \varphi(A_2, A_1, A_3, \dots, A_n) + \varphi(A_2, A_2, A_3, \dots, A_n). \end{aligned}$$

Using the fact that φ is alternating, we are left with

$$0 = \varphi(A_1, A_2, A_3, \dots, A_n) + \varphi(A_2, A_1, A_3, \dots, A_n),$$

which proves that a switch of the first two coordinates results in a change of sign (which is what we expected as $\mathrm{sgn}((1\,2)) = -1$).
It can be checked in the same way as done over fields that the function det is alternating and multilinear, and that it satisfies the Lagrangian expansion in the first column: for $A = (a_{ij})$,

$$(**) \quad \det(A) = \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det(A'(i,1))$$

where $A'(i,j)$ is the matrix obtained by deleting the i-th column and the j-th row from A.
Now we prove the following statement by induction on n

(***) If $\varphi : M^n \longrightarrow R$ is alternating multilinear, then $\varphi(A) = \varphi(\mathrm{Id}_n)\det(A)$.

The statement is clear for $n = 1$, because $\varphi(a) = a\varphi(1)$. Now suppose that (***) holds for $n-1$ and let us prove it holds for n. Let $E_1, \dots, E_n \in M$ be the columns defined by $E_j = (\delta_{ij})_{1 \leqslant i \leqslant n}$. For $B = (b_i) \in M$, we can write

$$B = \sum_{i=0}^{n} b_i E_i.$$

For $A = (A_1, A_2, \dots, A_n)$, with $A_j = (a_{ij})_i$, we can write by multilinearity:

$$\varphi(A) = \sum_{i=1}^{n} a_{i1} \varphi(E_i, A_2, \dots, A_n) \tag{2}$$

One can prove with a simple recursion that

$$\varphi(E_i, A_2, \dots, A_n) = \varphi(E_i, A_2 - a_{i2}E_i, \dots, A_n - a_{in}E_i), \tag{3}$$

because φ is alternating multilinear so that we can add to any column a multiple of another column without changing the value of φ. Consider the map $\theta_i : R^{(n-1)^2} \longrightarrow R^{n^2}$ sending B to the unique matrix $\theta_i(B) = (c_{\lambda,\mu}) \in M^n$ such that

- $(\theta_i(B))'(i,1) = B$;
- the first column of $\theta_i(B)$ is E_i;
- the i-th row of $\theta_i(B)$ is $(1, 0, \dots, 0)$.

One can easily check that the function $\varphi \circ \theta_i : R^{(n-1)^2} \longrightarrow R$ is an alternating multilinear form, so that by inductive hypothesis $\varphi \circ \theta_i = \varphi(\theta_i(\mathrm{Id}_n)) \det$. Since the matrix $(E_i, A_2 - a_{i2}E_i, \ldots, A_n - a_{in}E_i)$ in the argument of φ on the right hand side of (3) is $\theta_i(A'(i,1))$, (3) gives

$$\begin{aligned}\varphi(E_i, A_2, \ldots, A_n) = \varphi(\theta_i(\mathrm{Id}_{n-1})) \det(A'(i,1)) = \\ &= \varphi(E_i, E_1, \ldots, E_{i-1}, E_{j+1}, \ldots, E_n) \det(A'(i,1)) \\ &\overset{(*)}{=} (-1)^{i-1}\varphi(E_1, \ldots, E_{i-1}, E_i, E_{j+1}, \ldots, E_n) \det(A'(i,1)) \\ &=(-1)^{i+1}\varphi(\mathrm{Id}_n) \det(A'(i,1)).\end{aligned}$$

By (2), we deduce that

$$\varphi(A) = \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \varphi(\mathrm{Id}_n) \det(A'(i,1)) \overset{(**)}{=} \varphi(\mathrm{Id}_n) \det(A),$$

proving (***).
We now make the following claim:

(****) $B \mapsto \det(AB)$ is an alternaring multilinear form on M^n for all $A \in M^n$.

If the claim holds, then for each $A, B \in M^n$ we know by (***) that

$$\det(AB) = \det(A \cdot \mathrm{Id}_n) \det(B) = \det(A) \det(B),$$

proving the multiplicativity of the determinant.
In order to prove (****) let $f_A : M^n \longrightarrow R$ be the map $f_A(B) = \det(AB)$. For $B \in M^n$, write $B = (B_1, \ldots, B_n)$. Then $AB = (AB_1, \ldots, AB_n)$. An equality $B_i = B_j$ implies $AB_i = AB_j$. Moreover, the map $M \longrightarrow M$ sending $X \mapsto AX$ is linear. Since det is an alternating multilinear form, it easily follows that f_A is an alternating linear form, too, proving (****), the last remaining claim to prove for the multiplicativity of the determinant.
In order to conclude, we prove the characterization of invertible matrices in terms of the determinant. Suppose that $A \in R^{n^2}$ is invertible and let $B \in R^{n^2}$ be such that $AB = \mathrm{Id}_n$. Then $1 = \det(\mathrm{Id}_n) = \det(AB) = \det(A)\det(B)$, so that $\det(A) \in R^\times$—it has inverse B. Conversely, it can be proven as done over fields in Linear Algebra that, denoting by $C(A)$ the matrix of cofactors of A, there is an equality $C(A)^T A = AC(A)^T = \det(A)\mathrm{Id}_n$, so that if $\det(A) \in R^\times$ the matrix $\det(A)^{-1}C(A)^T$ is an inverse of A.

5. Show that $\mathbb{Q}$ is a $\mathbb{Z}$-module without torsion, that it is not finitely generated and not free.

   Solution: The $\mathbb{Z}$-module $\mathbb{Q}$ has no torsion, because the ring $\mathbb{Q}$ is an integral domain, so that for $m \in \mathbb{Z} \smallsetminus \{0\}$ and $q \in \mathbb{Q} \smallsetminus \{0\}$ we know that $m \cdot q \neq 0$. This means that $\mathbb{Q}$ has no $\mathbb{Z}$-torsion.

Given a finite set of rational numbers $F = \{\frac{a_1}{b_1}, \dots, \frac{a_m}{b_m}\}$ for $a_j \in \mathbb{Z}$ and $b_j \in \mathbb{Z}_{>0}$, for every $q \in \langle F \rangle$, we notice that $Nq \in \mathbb{Z}$ for $N = \prod_{j=1}^{m} b_j$. Hence $\langle F \rangle \subset \frac{1}{N}\mathbb{Z}$, which is strictly smaller than $\mathbb{Q}$ (for example, it does not contain $\frac{1}{N^2}$. This implies that $\mathbb{Q}$ is not finitely generated.

Given $q_1, q_2 \in \mathbb{Q} \setminus \{0\}$, there exist $\lambda_1, \lambda_2 \in \mathbb{Z} \setminus \{0\}$ such that $\lambda_1 q_1 = \lambda_2 q_2$. This implies that each two non-zero elements of $\mathbb{Q}$ are not linear independent. If $\mathbb{Q}$ were free, the free generating set of $\mathbb{Q}$ over $\mathbb{Q}$ would necessarily contain only 1 element, contradicting the fact that $\mathbb{Q}$ is not finitely generated. Hence $\mathbb{Q}$ is not free.

6. Let K be a finite field of cardinality $q = p^n$ for some prime $p \neq 2$. Suppose that $\varepsilon \in K^\times$ is not a square in K. Define

$$T = \left\{ \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} \right\} \subset \mathrm{GL}_2(K).$$

   (a) Show that T is an abelian subgroup of $\mathrm{GL}_2(K)$.

   (b) Show that T is isomorphic to $L^\times$ where L is the unique extension of K of degree 2.

   (c) For $x = \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} \in T$, prove that

$$x^q = \begin{pmatrix} a & -b \\ -b\varepsilon & a \end{pmatrix}.$$

Solution:

   (a) Notice that T contains the identity matrix so it is non-empty. For $x = \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} \in T$ and $x' = \begin{pmatrix} a' & b' \\ b'\varepsilon & a' \end{pmatrix} \in T$, we see that

$$\begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} \begin{pmatrix} a' & b' \\ b'\varepsilon & a' \end{pmatrix} = \begin{pmatrix} aa' + bb'\varepsilon & ab' + a'b \\ (ab' + a'b)\varepsilon & aa' + bb'\varepsilon \end{pmatrix} \in T$$

   and that switching $a \leftrightarrow a'$ and $b \leftrightarrow b'$ the result does not change, so that multiplication in T is closed and commutative. Moreover, the inverse of x is

$$x^{-1} = \frac{1}{a^2 - \varepsilon b^2} \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} \in T$$

   and we can conclude that T is an abelian subgroup of $\mathrm{GL}_2(K)$.

   (b) Let $T_0 = T \cup \{0\} \subset K^{2\times 2}$. It is clear that T_0 is closed under sum and multiplication of matrices, and that both operations are commutative in T_0. It contains the matrices 0 and 1 and it is closed under taking the opposite of a matrix. Hence it is a commutative subring of the (non-commutative) ring $K^{2\times 2}$. By part (a), $T_0^\times = T$, so that T_0 is a field. Notice that for each $(a,b) \in K^2 \smallsetminus \{(0,0)\}$, the matrix $x = \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix}$ has determinant $a^2 - \varepsilon b^2 \neq 0$, because the equality $a^2 = \varepsilon b^2$ cannot hold since ε is not a square in K. Hence

$$\mathrm{Card}(T_0) = 1 + \mathrm{Card}(T) = 1 + (q^2 - 1) = q^2.$$

This implies that T_0 is a field of q^2 elements and as such it is isomorphic to L, the unique subfield of $\overline{K}$ with cardinality q^2. This isomorphism restricts to an isomorphism of the multiplicative groups $T \cong L^\times$.

(c) The field K identifies with the subfield of T_0 consisting of scalar matrices. Under this identification, for $\alpha = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$, we can write $x = x^q = \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} = a + b\alpha$. Then x is a root of $\mathrm{irr}(x, K) = (X - a)^2 - \varepsilon b^2$ and by Exercise 2(b) x^q is the other root of this polynomial, that is, $x^q = a - b\alpha$. Hence

$$x^q = \begin{pmatrix} a & -b \\ -b\varepsilon & a \end{pmatrix}.$$