# Solutions of exercise sheet 12

The content of the marked exercises **(*)** should be known for the exam.

**1. (*)** Let $p$ be a prime number and $n$ a positive integer. For each element $x \in \mathbb{F}_{p^n}$, we define its trace and norm over $\mathbb{F}_p$ as

$$\operatorname{Tr}(x) = \sum_{j=0}^{n-1} x^{p^j} \quad \text{and} \quad \operatorname{N}(x) = \prod_{j=0}^{n-1} x^{p^j}.$$

Check the following properties:

- For each $x \in \mathbb{F}_{p^n}$, both $\operatorname{Tr}(x)$ and $\operatorname{N}(x)$ lie in $\mathbb{F}_p$;
- The map $\operatorname{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is $\mathbb{F}_p$-linear;
- The map $\operatorname{N} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is multiplicative (i.e, $\operatorname{N}(xy) = \operatorname{N}(x)\operatorname{N}(y)$), and $\operatorname{N}(x) = 0$ if and only if $x = 0$.

[Actually, these definitions of trace and norm agree with the more general ones we gave in Exercise 3 from Exercise sheet 11].

**Solution:**

- As seen in class, for $\alpha \in \mathbb{F}_{p^n}$, we have that $\alpha \in \mathbb{F}_p$ if and only if $\alpha^p = \alpha$. Hence we only need to show that the trace and the norm of $x \in \mathbb{F}_{p^n}$ do not change under taking the $p$-th power. We know that $x \mapsto x^p$ is an endomorphism of $\mathbb{F}_{p^n}$ (called the Frobenius endomorphism), so that it respects sums, and

$$(\operatorname{Tr}(x))^p = \left(\sum_{j=0}^{n-1} x^{p^j}\right)^p = \sum_{j=0}^{n-1} \left(x^{p^j}\right)^p = \sum_{j=0}^{n-1} \left(x^{p^{j+1}}\right) = \sum_{j=0}^{n-1} \left(x^{p^{j+1}}\right) =$$
$$= \sum_{j=1}^{n} \left(x^{p^j}\right) = \sum_{j=0}^{n-1} \left(x^{p^j}\right) = \operatorname{Tr}(x),$$

where we have used the fact that $x^{p^n} = x$ since $x \in \mathbb{F}_{p^n}$. Hence $\operatorname{Tr}(x) \in \mathbb{F}_p$ for each $x \in \mathbb{F}_{p^n}$. The same computation with a product instead of a sum gives that $\operatorname{N}(x)^p = \operatorname{N}(x)$ for $x \in \mathbb{F}_{p^n}$, so that $\operatorname{N}(x) \in \mathbb{F}_p$.

**Please turn over!**

- By definition, we have that $\mathrm{Tr} = \sum_{j=0}^{n-1} \varphi^j$, where $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is the Frobenius field endomorphism sending $x \mapsto x^p$, and $\varphi^j$ is its $j$-th iteration. Since $\varphi$ fixes $\mathbb{F}_p$ and respects multiplication, it is an $\mathbb{F}_p$-linear map. Thus Tr is also $\mathbb{F}_p$-linear, as it is a sum of compositions of $\mathbb{F}_p$-linear maps $\mathbb{F}_p \to \mathbb{F}_p$ (for $j = 0$, $\varphi^0$ is the identity of $\mathbb{F}_{p^n}$, which is also $\mathbb{F}_p$-linear).
- For $x, y \in \mathbb{F}_{p^n}$, we have

$$\mathrm{N}(xy) = \prod_{j=0}^{n-1} (xy)^{p^j} = \prod_{j=0}^{n-1} x^{p^j} y^{p^j} = \prod_{j=0}^{n-1} x^{p^j} \prod_{j=0}^{n-1} y^{p^j} = \mathrm{N}(x)\mathrm{N}(y),$$

so that N is a multiplicative map. Moreover, since for $x \in \mathbb{F}_{p^n}$ one has $\mathrm{N}(x) = x^{\sum_{j=0}^{n-1} p^j}$ and $\mathbb{F}_{p^n}$ is a field (and hence an integral domain), we have that $\mathrm{N}(x) = 0$ if and only if $x = 0$.

**2.** For $K$ a field and $n$ a positive integer, we define $\mathrm{GL}_n(K)$ to be the multiplicative group of invertible square matrices of order $n$ with coefficients in $K$. It is isomorphic to the automorphism group of the $K$-vector space $K^n$.

1. For $K$ a finite field of $q$ elements, prove that the cardinality of $\mathrm{GL}_n(K)$ is

$$|\mathrm{GL}_n(K)| = \prod_{j=0}^{n-1} (q^n - q^j).$$

2. For $|K| = q$ as before, and $q = p^r$ for some prime $p$ and positive integer $r$, show that a $p$-Sylow subgroup of $\mathrm{GL}_n(K)$ is given by the group of upper triangular matrices with one on the diagonal,

$$H_n(K) = \left\{ \begin{pmatrix} 1 & a_{1,2} & \dots & a_{1,n} \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ 0 & \dots & 0 & 1 \end{pmatrix} : a_{i,j} \in K \right\}.$$

**Solution:**

1. By basic linear algebra, we have that a matrix $A \in M_n(K)$ is invertible if and only if its columns, interpreted as vectors in $K^n$, are linearly independent. Hence $|GL_n(K)|$ is the number of ordered $n$-tuples of $K$-linearly independent vectors in $K^n$. This can be found inductively by counting the number $N_k$ of ordered $k$-tuples of $K$-linearly independent vectors in $K^n$, for $0 \le k \le n$. We claim that

$$N_k = \prod_{j=0}^{k-1} (q^n - q^j),$$

which for $k = n$ gives indeed the desired cardinality.

**See next page!**

We prove the claim $N_k = \prod_{j=0}^{k-1}(q^n - q^j)$ by induction on $0 \leq k \leq n$. For $k = 0$, we have $\prod_{j=0}^{k-1}(q^n - q^j) = 1$ (the empty product), and there is indeed one 0-tuple of $K$-linearly independent vectors, that is, the empty tuple. If this does not satisfy the reader, they can notice that $N_1 = |K^n| = q^n$, which coincides with $\prod_{j=0}^{1-1}(q^n - q^j)$. To conclude, suppose that $N_{k-1} = \prod_{j=0}^{k-2}(q^n - q^j)$. Now we have that each $k$-tuple of $K$-linear independent vectors consists of one of the $N_{k-1}$ $(k-1)$-tuple of $K$-linear independent vectors, followed by a vector which does not lie in the span of the previous $k-1$ vectors. Since $k-1$ linearly independent vectors span over $K$ precisely $q^{k-1}$ vectors, while $|K^n| = q^n$, the $k$-th vector can be chosen among $(q^n - q^{k-1})$, and we obtain

$$N_k = N_{k-1}(q^n - q^{k-1}) = \prod_{j=0}^{k-1}(q^n - q^j),$$

proving the inductive step.

2. From the previous point, we have

$$|\operatorname{GL}_n(K)| = q^{\binom{n}{2}} \prod_{j=0}^{n-1}(q^{n-j} - 1),$$

where the product is not divisible by $p$ (as $p$ is prime and none of the factor is divisible by $p$, since they are congruent to $-1$ modulo $p$), while $q^{\binom{n}{2}}$ has $p$ as unique prime factor. Hence a $p$-Sylow subgroup of $\operatorname{GL}_n(K)$ contains precisely $q^{\binom{n}{2}}$ elements. The given set $H_n(K)$ consists of invertible matrices (as they have determinant 1), and its cardinality is $q^l$, where $l$ is the number of elements in the upper triangle which do not lie in the principal diagonal. We obtain that $l = (n^2 - n)/2 = \binom{n}{2}$, so that $H_n(K)$ has the cardinality of a $p$-Sylow subgroup of $\operatorname{GL}_n(K)$. To conclude, we just notice that $H_n(K)$ is indeed a subgroup of $\operatorname{GL}_n(K)$. This is because the determinant of its matrices is always 1, so that for $A \in H_n(K)$ we have that $A^{-1}$ is the transpose of the matrix of cofactors. Since the cofactor matrix is easily seen to be lower-triangular with 1 in the diagonal, we can conclude that $A^{-1}$ is still in $H_n(K)$. Moreover, $H_n(K)$ is closed by multiplication, as one can immediately check with the formulas for the coefficients of the product of two matrices.

**3.** Let $G$ be a finite group and $V, W \subseteq G$ subsets such that $|V| + |W| > |G|$. Prove: $G = VW$. [*Hint:* For $g \in G$, the sets $V$ and $gW^{-1}$ need to intersect.]

**Solution:**

Fix $g \in G$. We want to prove that $g = vw$, for some $v \in V$ and $w \in W$. Since the map $G \to G$ sending $x \mapsto gx^{-1}$ is a bijection (whose inverse is indeed $y \mapsto y^{-1}g$), we have that $|gW^{-1}| = |W|$. Now

$$|G| < |V| + |g^{-1}W| = |V \cup gW^{-1}| + |V \cap gW^{-1}| \leq |G| + |V \cap gW^{-1}|,$$

which implies that $V \cap gW^{-1} \neq \varnothing$. Then there exists $v \in V$ such that $v = gw^{-1}$ for some $w \in W$, which gives $g = vw$.

**4.** Let $F$ be a finite field. We say that $x \in F$ is a square in $F$ if there exists $y \in F$ such that $y^2 = x$.

1. Suppose that $\operatorname{char}(F) = 2$. Prove that every element of $F$ is a square in $F$.
2. Now suppose that $\operatorname{char}(F) = p \geq 3$. Let

$$S = \{\alpha \in F \mid \exists b \in F : \alpha = b^2\} \text{ and } S' = S \setminus \{0\}.$$

   Prove:
   - $S'$ is a subgroup of index 2 of $F^\times$ [*Hint:* the map $x \mapsto x^2$ of $F^\times$ is not injective];
   - $2 \cdot |S| > |F|$.
3. Deduce that for every finite field $F$, every element in $F$ can be expressed as the sum of two squares in $F$. [*Hint:* Previous exercise.]
4. Let $F = \mathbb{F}_p$ with $p \geq 3$. Prove that $-1 \in \mathbb{F}_p$ is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.

**Solution:**

In the following, we will denote by $\alpha$ the map $F \to F$ sending $x \mapsto x^2$. This is a multiplicative map (as $F$ is a commutative ring) sending $0 \mapsto 0$ and $1 \mapsto 1$.

1. If $\operatorname{char}(F) = 2$, we have that $\alpha : x \mapsto x^2$ is a field endomorphism of $F$, as for $x, y \in F$ we have $(x+y)^2 = x^2 + y^2 + 2xy = x^2 + y^2$. Then $\alpha$ is injective because it has trivial kernel ($x^2 = 0$ if and only if $x = 0$, as $F$ is a field), and being $F$ finite $\alpha$ needs to be surjective as well. In conclusion, $\operatorname{Im}(\alpha) = F$, that is, every element in $F$ is a square in $F$.
2. - The map $\alpha' := \alpha|_{F^\times}$ is a group endomorphism of $F^\times$, so that $S' = \operatorname{Im}(\alpha')$ is a subgroup of $F^\times$, whose index coincides with $|\ker(\alpha')|$ by the First Isomorphism Theorem for groups. We have that $\ker(\alpha')$ is the set of roots in $F$ of the polynomial $X^2 - 1 = (X-1)(X+1)$, that is, $\ker(\alpha') = \{\pm 1\}$, so that, 1 and $-1$ being distinct when $\operatorname{char}(F) \neq 2$, we have $[F^\times : S'] = |\ker(\alpha')| = 2$.
   - By definition, $|S| = |S'| + 1$. Moreover, we have just proven that $|S'| = \frac{1}{2}|F^\times| = \frac{1}{2}(|F| - 1)$. Putting everything together, we can conclude that

$$2 \cdot |S| = 2 \cdot |S'| + 2 = |F| - 1 + 2 > |F|.$$

3. As fields of characteristic zero contain a copy of $\operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$, all finite fields have positive characteristic. If $\operatorname{char}(F) = 2$, part 1 proves that every element in $F$ is a square, and in particular every element is a sum of two squares. If $\operatorname{char}(F) \geq 3$, using the notation of part 2 we need to prove that $S + S = F$. This follows immediately from the previous exercise, by taking the additive group $F$ and the subsets $V = W = S$, so that $|S| + |S| > |F|$ as we proved.

**See next page!**

4. Let $F = \mathbb{F}_p$, and let us denote by $F^{\times 2}$ the set of invertible squares in $F$. As seen in class, we have that for each $a \in \mathbb{F}_p$ one has $a^p = a$, so that for each $a \in F^\times$ one has $a^{p-1} = 1$. This means that $F^\times$ is the set of roots of the polynomial $f_p(X) = X^{p-1} - 1$. This polynomials factors (since $2|p-1$) as

$$f_p(X) = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1).$$

Suppose that $c \in F^{\times 2}$, with $c = b^2$ and $b \neq 0$. Then

$$c^{\frac{p-1}{2}} = b^{p-1} = 1,$$

so that $c$ is a root of the factor $(X^{\frac{p-1}{2}} - 1)$. By point 2, we have that $|F^{\times 2}| = (p-1)/2$, and this implies that the for each $a \in F^\times$ one has

$$\begin{aligned} a \in F^{\times 2} &\iff a^{\frac{p-1}{2}} = 1, \\ a \notin F^{\times 2} &\iff a^{\frac{p-1}{2}} = -1. \end{aligned}$$

Now we apply this for $a = -1$. We have that $p$ is odd, so that we can write $p = 2k+1$. Then $\frac{p-1}{2} = k$. If $k$ is even, then $(-1)^{\frac{p-1}{2}} = 1$, so that $-1$ is a square in $F$. If $k$ is odd, then $(-1)^k = -1$, so that $-1$ is not a square in $F$. Since $k$ is even if and only if $p \equiv 1 \pmod 4$, we can conclude that, for $p \geq 3$, $-1$ is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.