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

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

Check the following properties:

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

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

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,

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

Please turn over!

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.]

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 $\mathrm{char}(F) = 2$. Prove that every element of F is a square in F.
2. Now suppose that $\mathrm{char}(F) = p \geq 3$. 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 $p \equiv 1 \pmod 4$.

Due to: 11 December 2014, 3 pm.