Math40003 Linear Algebra and Groups, Term 2 Unseen 5 (week 8)

1. Suppose $q, n \in \mathbb{N}$ and $\mathbb{F}_q$ is a field with q elements.

   (a) Find a formula (depending on n and q) for the number of bases $v_1, \dots, v_n$ of $\mathbb{F}_q^n$ (consider choosing $v_1, v_2, \dots$ in turn).

   (b) What is the order of $GL_n(\mathbb{F}_q)$, the group of all invertible $n \times n$ matrices over $\mathbb{F}_q$.

   For the rows of A to be linearly independent, we can choose as the first row any non-zero vector in $\mathbb{F}_q^n$. For the $k+1^{th}$ rows, we need to exclude all vectors in the span of the first k rows. Assuming the first k rows $r_1, \dots, r_k$ are l.i., different choices of $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$ yield different vectors $\alpha_1 r_1 + \dots + \alpha_k r_k$. So there is a bijection between $\mathbb{F}_q^k$ and $\text{span}(r_1, \dots, r_k)$. Any choice of vector from $\mathbb{F}_q^n \setminus \text{span}(r_1, \dots, r_k)$ is valid for r_{k+1} and no else. So there are $q^n - q^k$ options for the $k+1$ vector. In conclusion, choosing n rows we have

   $$(q^n - 1) \cdot (q^n - q) \cdot \dots \cdot (q^n - q^{n-1}) = \prod_{i=0}^{n-1} (q^n - q^i).$$

   (c) Suppose $0 \neq \alpha \in \mathbb{F}_q$. Show that the number of matrices in $GL_n(\mathbb{F}_q)$ with determinant α does not depend on the choice of α. When do these matrices form a subgroup of $GL_n(\mathbb{F}_q)$?

   (d) Find a formula (depending on n and q) for the order of $SL_n(\mathbb{F}_q)$, the group of all $n \times n$ matrices over $\mathbb{F}_q$ with determinant 1.

   For $k \in \mathbb{F}_q \setminus \{ 0 \}$, let A_k be the set of $n \times n$ matrices of determinant k. So A_k are disjoint, $\bigcup_{i=1}^{q} A_i = GL_n(\mathbb{F}_q)$ and $A_1 = SL_n(\mathbb{F}_q)$. Let $f_j : A_1 \to A_k$ be the map defined such that $f(M)$ is achieved by multiplying the first row of M by k. Let $g_j : A_k \to A_1$ be the map defined such that $f(M)$ is achieved by multiplying the first row of M by k^{-1}. Then $f \circ g = Id_{A_k}$ and $g \circ f = Id_{A_1}$, so f_k is a bijection. Therefore $|A_i| = |A_j|$ for all $i, j \in \mathbb{F}_q \setminus \{ 0 \}$. So

   $$|A_i| = |GL_n(\mathbb{F}_q)| / |\mathbb{F}_q \setminus \{ 0 \}| = \frac{\prod_{i=0}^{n-1} (q^n - q^i)}{q - 1}.$$

2. Let $(G, .)$ be a finite group and let $A, B \subseteq G$ be subsets. Prove that if $|A| + |B| > |G|$ then $G = AB$ where $AB = \{ a.b | a \in A, b \in B \}$

   First notice that if $|A| + |B| > |G|$, then $A \cap B \neq \emptyset$. Notice that

   $$g \in A * B \iff 1 \in g^{-1} \star A \star B \iff (g^{-1} \star A) \cap B^{-1} \neq \emptyset,$$

where $B^{-1} = \{ b^{-1} | b \in B \}$ and $g^{-1} \star A = \{ g^{-1} * a | a \in A \}$. Notice also that $|g^{-1} * A| = |A|$ and $|B^{-1}| = |B|$, so $|g^{-1} * A| + |B^{-1}| > |G|$, therefore $(g^{-1} \star A) \cap B^{-1} \neq \emptyset$.

3. Let F be a finite field. Prove that every element of F is a sum of two squares, i.e., for every $a \in F$, there are $b_1, b_2 \in F$ such that $a = b_1^2 + b_2^2$. Is it true that every $n \in \mathbb{N}$ is a sum of two squares of $\mathbb{N}$?

   By Question 2, It suffices to show that $F^2 = \{ a^2 | a \in F \}$ is of size $> |F|/2$. It was proved in Question Sheet 2, Q4, that every polynomial $x^2 - a$ has at most 2 roots, there for the map $f : F \to F$ defined by $f(x) = x^2$ is $\leq 2 - to - 1$, i.e., for every $a \in F$, there are at most two b's such that $f(b) = a$. So $|(F^\times)^2| \geq |F^\times|/2$. For 0, the only b such that $f(b) = 0$ is 0. So $|F^2| = |(F^\times)^2| + 1 \geq |F^\times|/2 + 1$. Therefore, $|F^2| > |F|/2$.

4. Let X be a set and let $G \leq Sym(X)$ be a subgroup. G *acts freely* if $\forall x \in X$, $g, h \in G$: $g(x) = h(x) \Longrightarrow g = h$. G *is transitive* if $\forall x, y \in X$, $\exists g \in G$: $g(x) = y$. Prove that if G is transitive and acts freely, then $|G| = |X|$.

   Fix some $x_0 \in X$ and let $\phi : G \to X$ be defined as $\phi(g) := g(x_0)$. Free action and transitivity give injectivity and surjectivity, respectively.