HANDOUT (ΛICTOK) 1

A.A.KIRILLOV

In the Spring semester of 2019 I will teach at HSE the course

"Topics in the modern representation theory. The orbit method for the triangular group over a finite field."

The text below is the first handout to this course. Due to technical reasons, it is written in English. The next ones will be in Russian.

1. Finite fields

1.1. **Motivation.** In my book "What is number?" (Moscow, 1992) I tried to describe which objects can play the role of numbers in mathematics.

Besides the standard variants $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ (i.e. natural numbers, integers, rational, real, complex numbers and quaternions), there are several other remarkable possibilities. One of them we describe here.

Consider a *finite field*, i.e., a finite set F, where all four arithmetical operations (addition, subtraction, multiplication and division by non-zero elements) are defined and satisfy ordinary conditions (commutativity, associativity and distributivity laws, existence of neutral elements for addition and multiplication).

Call elements of F *numbers* and try to develop the main mathematical theories: analysis, algebra, geometry, etc in this situation.

1.2. **First examples.** To show that our theories make sense, we must, first of all, to give the examples of such sets F. The simplest possible example is a one-element set $\mathbb{F}_1$ with the only element $a \in \mathbb{F}_1$, satisfying $a + a = a - a = a \cdot a = a/a = a$. This example seems to be not very interesting. Therefore, an attempt was made to exclude this field from consideration. Some algebraists introduced the special axiom: the two neutral elements (0 for addition and 1 for multiplication) can not coincide.[1]

The next example is the two-element set $\mathbb{F}_2 = \{0, 1\}$ with operations

$$\begin{array}{cc} 0+0=0 & 0\cdot 0=0 \\ 0+1=1+0=1 & 0\cdot 1=1\cdot 0=0 \\ 1+1=0 & 1\cdot 1=1. \end{array}$$

Date: Jan 2019.

[1]But in the mathematics the method of brute force does not work. Recently a very interesting new theories were invented, where the field $\mathbb{F}_1$ plays an essential role. See e.g. the paper by J. Soulé.

This example is well-known as the ring of residues modulo 2 (or classes of even and odd integers). This ring $\mathbb{Z}/2\mathbb{Z}$ is actually a field! Moreover, you can show (can you?), that any finite field with two elements is isomorphic to $\mathbb{F}_2$ (can you formulate what does it mean?)

Quizz 1. For which $n \in \mathbb{N}$ the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field? (I.e., all non-zero elements of the ring are invertible?)

The ring $\mathbb{Z}/4\mathbb{Z}$ is not a field (why?) But a field F with four elements does exist. It contains $\mathbb{F}_2$ as a subfield $\{0\ 1\}$. Hence, F is a vector space over $\mathbb{F}_2$. The dimension of this vector space must be two, and a basis consists of two elements. We can take the multiplicative unit 1 as one of them and denote by x the second one. Then the four elements of F will be 0, 1, x, $1+x$. The multiplication table for basic elements must have the form

$1 \cdot 1 = 1$	$1 \cdot x = x$
$x \cdot 1 = x$	$x \cdot x = a + bx$

Quizz 2. a) Find all possible values for the coefficients a, $b \in \mathbb{F}_2$ and show that all fields F, obtained in this way are isomorphic to one field, which we denote $\mathbb{F}_4$.

b) Find the realization of $\mathbb{F}_4$ as a subalgebra of the matrix algebra $\mathrm{Mat}_2(\mathbb{F}_2)$.

1.3. **Main facts.** The main properties of finite fields we formulate in the

Theorem 1. *a) A field F with q elements exists iff q has the form $q = p^k$ where p is a prime number and $k \in \mathbb{N}$.*

b) All fields with q elements are isomorphic to one field, denoted $\mathbb{F}_q$.

c) The field $\mathbb{F}_q$, $q = p^k$, can be realized as a subalgebra of the matrix algebra $Mat_k(\mathbb{F}_p)$.

d) The multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$ is cyclic, hence, isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$.

We split the proof in the series of exercises.

1. Let 1 be the multiplicative unit in F. Put $S_k := \overbrace{1+1+\cdots+1}^{k \text{ terms}}$. Show that there is a prime number p such that $S_k = 0$ iff k is divisible by p. This number is called the *characteristic* of the field F.

Hint: Let n be the minimal natural number such that $S_n = 0$. Then n must be prime, since if $n = n_1 n_2$, $n_i > 1$, then $S_{n_1} \neq 0$ and $S_{n_2} \neq 0$. Hence, $S_n = S_{n_1} \cdot S_{n_2} \neq 0$. A contradiction.

2. Show that any field F of characteristic p contains the subfield, isomorphic to $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Thus, any field F of characteristic p can be considered as a vector space over $\mathbb{F}_p$. For every $x \in F$ we denote by M_x the operator of multiplication by x in F. Clearly, it is a linear operator over $\mathbb{F}_p$. The

correspondence $x \mapsto M_x$ gives the desired realization of F. We denote $\operatorname{tr} M_x$ simply by $\operatorname{tr} x$.

3. Möbius inversion formula. For any function $f : \mathbb{N} \to \mathbb{R}$ define the function $F : \mathbb{N} \to \mathbb{R}$ by

$$F(m) = \sum_{d|m} f(d), \quad \text{where } d|m \text{ means that } d \text{ is a divisor of } m. \tag{1}$$

Show that f can be expressed in terms of F by the formula

$$f(m) = \sum_{d|m} \mu(d) F(\frac{m}{d}), \tag{2}$$

where the Möbius function μ is defined by

$$\mu(m) = \begin{cases} (-1)^k & \text{if } m \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Hint. Consider first the case when f and F vanish outside the geometric progression $\{p^k\}_{k \in \mathbb{Z}_+} \subset \mathbb{N}$.

2. Maps between finite and other fields

2.1. **Additive and multiplicative groups.** Every field F gives rise two groups: the **additive group** $F^+ = (F, +)$ and **multiplicative group** $F^\times = (F \backslash \{0\}, \cdot)$. The first group is always abelian, the second can be non-abelian (e.g., quaternions); but for finite fields it is always cyclic, hence, abelian. We shall use also the dual groups $\widehat{F^+}$ and $\widehat{F^\times}$.

Introduce the notation

$$\mathbf{e}_p(k) = e^{2\pi i k/p} \quad \text{for } k \in \mathbb{F}_p.$$

For $F = \mathbb{F}_q$, $q = p^k$, we consider F as a vector space over $\mathbb{F}_p$. The general character of F^+ has the form

$$\chi_f(x) = \mathbf{e}_p(\langle f, x \rangle),$$

where f is a $\mathbb{F}_p$-linear functional on F. So, the dual group $\widehat{F^+}$ is isomorphic to F^*, the dual space to F. As an abstract group, it is the direct sum of k copies of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Among all $\mathbb{F}_p$-linear functionals on $\mathbb{F}_q$ we choose one. It is the trace of $x \in \mathbb{F}_q$, where x is realized as an operator of multiplication by x in $\mathbb{F}_q$. The corresponding character χ_{tr} of the group $(\mathbb{F}_q, +)$ we denote simply χ.

Now consider the multiplicative group $F^\times$ for $F = \mathbb{F}_q$. Denote the number $q-1$ by Q. Then $F^\times$ is isomorphic to the cyclic group $\mathbb{Z}/Q\mathbb{Z}$, but there is no canonical isomorphism. The role of generator can be played by any element of order Q in $F^\times$. The number of such element is given by the Euler **totient**

function $\phi(Q) = Q\prod_{p|Q}(1-\frac{1}{p})$. If s is a generator, the general multiplicative character has the form $\pi_m(s^k) = e^{2\pi i\frac{km}{Q}}$, where $gcd(k,\, m) = 1$.

2.2. **Fourier transform.** The Fourier transform in $\mathrm{Fun}(\mathbb{F}_q)$ is defined as

$$\widehat{f}(y) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} f(x)\overline{\chi_y(x)}. \tag{4}$$

An interesting example is the case when $f = \pi$, a multiplicative character of $\mathbb{F}_q$ (extended from $F^\times$ to F by the zero value at 0). We have:

$$\widehat{\pi}(\lambda y) = \tfrac{1}{q}\textstyle\sum_{x\in\mathbb{F}_q^\times}\pi(x)\overline{\chi_{\lambda y}(x)} = \tfrac{1}{q}\sum_{x\in\mathbb{F}_q^\times}\pi(x)\overline{\chi_y(\lambda x)}$$
$$\tfrac{1}{q}\textstyle\sum_{x\in\mathbb{F}_q^\times}\pi(\lambda^{-1}x)\overline{\chi_y(x)} = \tfrac{1}{q}\sum_{x\in\mathbb{F}_q^\times}\pi(\lambda^{-1})\pi(x)\overline{\chi_y(x)} = \pi^{-1}(\lambda)\widehat{\pi}(y).$$

So, the Fourier transform of π is proportional to the inverse character: $\widehat{\pi}(y) = c\cdot\pi^{-1}(y)$. The coefficient c in this formula depends on the multiplicative character π: $c = \widehat{\pi}(1) = \frac{1}{q}\sum_{x\in\mathbb{F}_q}\pi(x)\overline{\chi_1(x)}$ (So-called **Gauss sum**).

Compare these computation with their classical analogues for real field. Recall that the the classical additive and multiplicative characters are:

$$\text{for } F=\mathbb{R}:\ \chi_\lambda(x) = e^{i\lambda x},\ \lambda\in\mathbb{R},\quad \pi_{\alpha,\varepsilon}(x) = |x|^{i\alpha}(\operatorname{sgn}x)^\varepsilon,\ \alpha\in\mathbb{R},\ \varepsilon = 0,1;$$
$$\text{for } F=\mathbb{C}:\ \chi_\lambda(z) = e^{i\Re(\lambda z)},\ \lambda\in\mathbb{C},\quad \pi_{\alpha,n}(z) = |z|^{i\alpha}(\tfrac{z}{|z|})^n,\ \alpha\in\mathbb{R},\ n\in\mathbb{Z}.$$

The Fourier transform of a multiplicative character $\pi_{\alpha,\varepsilon}$ on $\mathbb{R}$ is defined by

$$\widehat{\pi_{\alpha,\varepsilon}}(y) = \int_{\mathbb{R}^\times}|x|^{i\alpha}(\operatorname{sgn}x)^\varepsilon e^{-ixy}dx. \tag{5}$$

It is a distribution on $\mathbb{R}$, satisfying $\widehat{\pi_{\alpha,\varepsilon}}(\lambda y) = |\lambda|^{-1}(\operatorname{sgn}\lambda)^\varepsilon\pi_{-\alpha,\varepsilon}(y)$. Hence, on $\mathbb{R}^\times$ it coincide with $c\cdot|y|^{-1}\pi_{-\alpha,\varepsilon}(y)$, where the constant

$$c = \int_{\mathbb{R}^\times}|x|^{i\alpha}(\operatorname{sgn}x)^\varepsilon e^{-ix}dx = \Gamma(1+i\alpha) + (-1)^\varepsilon\Gamma(1-i\alpha)$$

is expressed in terms of Euler Γ-function. Recall, that

$$\Gamma(1-i\alpha) = \overline{\Gamma(1+i\alpha)}\quad\text{and}\quad \Gamma(1+z)\Gamma(1-z) = \frac{\pi z}{\sin\,\pi z}.$$

2.3. **Relations between finite fields.** If p, p' are different primes, then there is no homomorphisms between $\mathbb{F}_q$ and $\mathbb{F}_{q'}$ for $q = p^k$, $q' = (p')^{k'}$.

Exercise 1. Show that a homomorphism $\alpha:\mathbb{F}_{p^m}\to\mathbb{F}_{p^n}$ exists iff $m|n$ (m is a divisor of n). In this case α is unique, is an embedding and its image consists of all $x\in\mathbb{F}_{p^n}$, satisfying $x^{p^m} = x$.

Exercise 2. Let p be a prime and $q = p^k$. a) Show that the **Frobenius map** $Fr\colon x \mapsto x^p$ is an automorphism of $\mathbb{F}_q$.

b) Show that the group $\mathrm{Aut}(\mathbb{F}_q)$ of all automorphisms of $\mathbb{F}_q$ is cyclic of order k with Fr as generator.

Exercise 3. Write the addition and multiplication tables for the fields $\mathbb{F}_q$ for $q = 3, 8, 9$.

Exercise 4. (Optional) Try to prove the uniqueness of $\mathbb{F}_q$, using the cyclic nature of $\mathbb{F}_q^\times$.

E-mail address: kirillov@math.upenn.edu