6320-001 - SPRING 2021 - WEEK 6 (2/23, 2/25)

1. This week in 6320

2/23 – Fourier theory
2/25 – Independence of characters
Key concepts: *Characters of finite groups, Fourier theory, independence of characters*

2. Comments and suggested reading

Characters in the sense discussed this week are simply one-dimensional representations of a group (i.e. homomorphisms $G \to \mathrm{GL}_1(L) = L^\times$ for G a finite group and L a field). Because $L^\times$ is abelian, any such map factors through G^{ab}, so it suffices to study characters of abelian groups. A warning about terminology – in the final few weeks of the class we will study higher dimensional representations (i.e. maps $G \to \mathrm{GL}_n(L)$); one also attaches something called a character to any such representation, but for $n \geq 2$ the character is something different from the representation itself (though, e.g., if $L = \mathbb{C}$ and G is finite, then it still uniquely determines the representation!).

Independence of characters is Theorem 7 in **DF**-14.2; it is an important technical ingredient in the proof of the fundamental theorem of Galois theory, which we will hit a few weeks after the midterm.

There is no suggested reading for this week.

3. Preview of next week

(This is subject to change depending on how far we get this week!)
Tuesday (3/02) will be a review, and the midterm will be in class on Thursday (3/04).

Midterm information: The midterm will be open-book and open-notes, but is to be taken individually and during the regular class period while logged on to Zoom. You will be put in individual breakout rooms so that you can call me in to ask any questions. If you are unable to take the midterm during class on 3/04 then please contact me ASAP.

The exam will consist of True/False and very-short answer questions. You will have one hour for the exam, then the remainder of the class will give you a buffer to submit either:
1) (preferred) upload to Gradescope a pdf or photo or scan of your ANSWERS ONLY
2) email to the instructor a pdf or photo or scan or plain text of your ANSWERS ONLY

4. Homework

Problem rewrites for homeworks 1-5 should be submitted via Gradescope by March 4th at 11:59pm. This week's homework does not have a "problem."

Due Tuesday, *March 16*, at 11:59pm on Gradescope Note: originally this assignment was planned to be due on March 2nd so that there would be no homework over "Spring Pause." Feel free to still turn it in early if you'd like! I extended the deadline to give you some more flexibility in how you budget your time; this did not effect the length of the assignment itself.
All solutions must be typeset using TeX and submitted via Gradescope; handwritten or late submissions will not be accepted. All exercises and problems submitted must start with the statement of the

exercise or problem.

You may work in groups, but you must write up your final solutions individually. Any instances of academic misconduct will be taken very seriously.

Justify your answers carefully!

4.1. **Exercises.** *Complete and turn in ALL exercises*:
Grading scale (for each part of an exercise):
3 points – A correct, clearly written solution
2 points – Right idea, but a minor mistake or not clearly argued
1 point – Some progress but multiple minor mistakes or a major mistake
0 points – Nothing written, totally incorrect, or no substantive progress made towards a solution.

Exercise 1. We fix an odd prime number p. In this exercise we will do some elementary computations (secretly motivated by basic ideas in Galois theory and representation theory) in order to obtain a formula for $\sqrt{p}$ as a $\mathbb{Z}$-linear combination of roots of unity in $\mathbb{C}$.

(1) Let $m(x) = \frac{x^p-1}{x-1} = x^{p-1} + \ldots + 1$. Show that $m(x) \in \mathbb{Q}[x]$ is irreducible. (Hint: use the Eisenstein criterion for irreducibility and the change of coordinates $x = t + 1$).

Let $L = \mathbb{Q}[x]/(m(x))$. Part (1) implies that $(m(x))$ is a maximal ideal in the principal ideal domain $\mathbb{Q}[x]$, thus L is a field. We write $\zeta \in L$ for the image of x under the quotient map.

(2) Show that $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are a basis for L as a $\mathbb{Q}$-vector space.
(3) Show that there is a unique ring homomorphism $L \to \mathbb{C}$ sending ζ to $e^{2\pi i/p}$ and that the image is the smallest subfield of $\mathbb{C}$ containing $e^{2\pi i/p}$.
(4) For each $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, show that there is a unique field automorphism

$$\sigma_k : L \xrightarrow{\sim} L$$

such that $\sigma_k(\zeta) = \zeta^k$.
(5) Use the uniqueness statement in (4) to show the map

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Aut}(K),\ k \mapsto \sigma_k$$

is a group homomorphism.
(6) Show that if $\ell \in L$ satisifies $\sigma_k(\ell) = \ell$ for all $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ then $\ell \in \mathbb{Q} \subset L$. (Hint: use the basis in (2), and the fact that $m(\zeta) = 0$ implies $\zeta + \zeta^2 + \ldots + \zeta^{p-1} = -1$).

In the following, you may use without proof that $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$.

(7) Show that there is a unique non-trivial character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, and that the kernel of χ consists of the squares in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Let

$$\tau = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(k)\sigma_k(\zeta) = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(k)\zeta^k \in L.$$

(8) Show that for any $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\sigma_k(\tau) = \chi(k)\tau$. (Hint: $\chi(k) = \chi(k)^{-1}$.)
(9) Show that for any $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\sigma_k(\tau^2) = \tau^2$, and deduce $\tau^2 \in \mathbb{Q}$.

(10) Using the the embedding $K \hookrightarrow \mathbb{C}$ from (3) and Euler's identity $e^{2\pi it} = \cos(t) + i\sin(t)$, to compute directly τ^2 when $p = 3$ and $p = 5$ (assuming the standard identities $\cos(\pm\pi/3) = -1/2$, $\cos(\pm\pi/5) = \frac{\sqrt{5}+1}{4}$, $\cos(\pm 2\pi/5) = \frac{\sqrt{5}-1}{4}$, and their counterparts for sin.)

In the remaining steps we will show $\tau^2 = -p$ if $p \equiv 3 \mod 4$ and $\tau^2 = p$ if $p \equiv 1 \mod 4$.

(11) Write $\alpha = \sum_{k\in(\mathbb{Z}/p\mathbb{Z})^\times} \sigma_k(\tau^2)$. Use (9) to deduce that $\alpha = (p-1)\tau^2$.
(12) Fill in the details of the following computations:

$$\begin{aligned}
\alpha &= \sum_{k\in(\mathbb{Z}/p\mathbb{Z})^\times} \sigma_k\left(\left(\sum_{s\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(s)\zeta^s\right)^2\right) \\
&= (p-1)^2\cdot\chi(-1) + \left(\sum_{a,b\in(\mathbb{Z}/p\mathbb{Z})^\times, a\neq -b} \chi(a)\chi(b)\right)\cdot(\zeta+\zeta^2+\ldots+\zeta^{p-1}) \\
&= (p-1)^2\cdot\chi(-1) + \left(\left(\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times}\chi(a)\right)^2 - \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times}\chi(a)\chi(-a)\right)\cdot(-1) \\
&= (p-1)^2\cdot\chi(-1) + (0-(p-1)\chi(-1))\cdot(-1) \\
&= (p-1)\cdot p\cdot\chi(-1).
\end{aligned}$$

(13) Conclude that $\tau^2 = -p$ if $p \equiv 3 \mod 4$ and $\tau^2 = p$ if $p \equiv 1 \mod 4$.
(14) Deduce that there is a $c \in \{\pm 1, \pm i\}$ such that, in $\mathbb{C}$,

$$\sqrt{p} = c\sum_{k=1}^{p-1}\chi(k)e^{\frac{2\pi ik}{p}},$$

where here $\sqrt{p}$ denotes the positive real square root of p.
Some remarks:

- *Step (7), suitably interpreted, is essentially "the Fourier transform of ζ evaluated at χ."*
- *We will see later that the map in (5) is an isomorphism, and then (6) is a special case of the fundamental identity in Galois theory: for L/K a Galois extension, $L^{\mathrm{Aut}(L/K)} = K$.*
- *Let us explain where this computation is coming from conceptually: Building on the previous point, the fundamental theorem of Galois theory tells us that there is a unique quadratic extension of $\mathbb{Q}$ contained in our field $L = \mathbb{Q}(\zeta)$. A combination of basic representation theory and Galois theory will tell us that we can use the formula in (7) to project any element of L into the space of square-roots generating this extension, and if we take a generator of L we are guaranteed to hit something nonzero. This is how we obtained an expression for a specific element generating this quadratic extension!*
- *If you develop a small amount of algebraic number theory, then there are more conceptual arguments that can replace the steps we took to compute τ^2.*
- *This result can be used to prove the quadratic reciprocity law.*
- *Bonus: determine c in (14).*