6370-001 - FALL 2021 - WEEK 7 (10/05, 10/07)

For any positive integer n and ring R, $\mu_n(R)$ denotes the group of nth roots of unity in R; $\mu(R) = \bigcup_n \mu_n(R)$ denotes all roots of unity in R.

Exercise 1. Let n be a positive integer. In this exercise you will show $\mathrm{Gal}(\mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$

1. Recall a simple proof of when n is a prime number. Why doesn't this work in general?
2. For K an algebraically closed field, describe $\mu_n(K)$ as an abstract group (be careful about characteristic!)
3. Use the complex exponential to construct an explicit isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n(\mathbb{C})$.
4. Give a *canonical* isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(\mu_n(\mathbb{C}))$, where $\mathrm{Aut}(\mu_n(\mathbb{C}))$ denotes the automorphisms of the group $\mu_n(\mathbb{C})$.
5. Show that $\mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q}$ is Galois, and show that restriction of a field automorphism to the subset $\mu_n(\mathbb{C})$ induces an injective group homomorphism
$$\mathrm{Gal}(\mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\mu_n(\mathbb{C})) = (\mathbb{Z}/n\mathbb{Z})^\times$$
6. Let $R = \mathbb{Z}[\mu_n(\mathbb{C})]$. Show that $\mu_n(R) = \mu_n(\mathbb{C})$, and that any element of $\mathrm{Gal}(\mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q})$ restricts to an automorphism of the ring R.
7. Let $\ell \nmid n$ be a prime number. For R as above, construct a map $\iota_\ell : R \to \overline{\mathbb{F}_\ell}$, and show that ι_ℓ restricts to an isomorphism of groups $\mu_n(R) = \mu_n(\overline{\mathbb{F}_\ell})$.
8. Deduce that for any $\ell \nmid n$ prime, $\ell \mod n$ is in the image of the injection from (4) (hint: suppose ζ is a generator for $\mu_n(\mathbb{C}) = \mu_n(R)$ – argue that ζ^ℓ is a factor of the minimal polynomial of ζ if and only if ℓ is in the image of the map of (4), then consider the factorization of the minimal polynomial mod ℓ and the action of the ℓ-power Frobenius automorphism on the roots in $\overline{\mathbb{F}_\ell}$ via a map ι_ℓ as above.)
9. Conclude that $\mathrm{Gal}(\mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercise 2. For p a prime number, we define the Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a nonzero square mod p} \\ -1 & \text{if } a \text{ is not a square mod } p \\ 0 & \text{if } p|a. \end{cases}$$

1. For $p \geq 3$, show $a \mapsto \left(\frac{a}{p}\right)$ is a surjective homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$. What's the kernel?

The quadratic reciprocity law says that for p and q distinct odd primes,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

We prove this as follows (below we identify $\mathrm{Gal}(\mathbb{Q}(\mu_p(\mathbb{C}))/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$):

2. Show -1 is a square mod q if and only if resp. q $\equiv 1$ mod 4.
3. Consider $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\mu_p(\mathbb{C}))$ (see Week 4 - Exercise 2). Use (1) to show that $q \in (\mathbb{Z}/p\mathbb{Z})^\times$ restricts to the trivial automorphism of $\mathbb{Q}(\sqrt{p^*})$ if and only if q is a square mod p.
4. Show that $q \in \mathbb{Z}/p\mathbb{Z}^\times$ induces the q-power Frobenius map $x \mapsto x^q$ on $\mathbb{Z}[\sqrt{p^*}]/q$.
5. Conclude.

This gives us a way to simplify $\left(\frac{n}{q}\right)$ for n a product of odd primes. To work for any n, we need:

6. Compute $\left(\frac{2}{q}\right)$ in terms of $q \mod 8$ (hint: consider $\mathbb{Q}(\mu_8(\mathbb{C}))$.)

Exercise 3. We will show the ring of integers in $K = \mathbb{Q}[\mu_p(\mathbb{C})]$ is $\mathbb{Z}[\mu_p(\mathbb{C})]$. (You may have already done this earlier, but here we spell out the final part of the argument in case you have not!).

1. First note that in the previous exercise this was never actually needed! If you used it at some point, go back and try to argue without it. Note that we also didn't use the full ring of integers in the quadratic extension $\mathbb{Q}(\sqrt{p^*})$ – why didn't that get us in trouble either?
2. Recall (or prove) that the discriminant of $\mathbb{Z}[\mu_p(\mathbb{C})]$ is $(-1)^{\frac{p-1}{2}}p^{p-2}$. Deduce that
$$\mathcal{O}_K[1/p] = \mathbb{Z}[1/p][\mu_p(\mathbb{C})].$$
3. Let $\zeta_p \in \mu_p(\mathbb{C})$ be a primitive pth root of unity. For $a \in \mathcal{O}_K$ use (2), to show that there is a minimal k such that
$$p^k a = a_0 + a_1(\zeta_p - 1) + \ldots + a_{p-2}(\zeta_p - 1)^{p-2}$$
for $a_i \in \mathbb{Z}$. Show $k = 0$ by using prime factorization of ideals in $\mathcal{O}_K$ (how does (p) factor?)

Exercise 4. We will need this unit computation in the next exercise.

1. For $n > 2$, show $L := \mathbb{Q}(\mu_n(\mathbb{C}))$ is a CM Field (see Week 6 - Exercise 5). Hint – show $K := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, for any primitive root ζ_n, is a totally real subfield and $[L : K] = 2$.
2. For $n = p$ an odd prime compute the ring of integers in the totally real subfield.
3. For $n = p$ an odd prime, show $\mathcal{O}_L^\times = \mu(L) \cdot \mathcal{O}_K^\times$ (Hint: see Week 6 - Exercise 5 to see what the other possibility is, then get a contradiction working mod $(1 - \zeta_p)$. See Prop 6.7 in Milne).

Exercise 5. A prime p is called regular if $p \nmid h_p$, where h_p is the class number of $\mathbb{Q}(\zeta_p)$. In this exercise, we show

Theorem (No case 1 solutions to the Fermat equation for regular primes)**.** *If $p \geq 3$ is a regular prime, then there are no integer solutions to $X^p + Y^p = Z^p$ such that $p \nmid XYZ$ and* $\gcd(X, Y, Z) = 1$.

The restriction to gcd 1 is just a convenience, as we can always factor out the gcd from an arbitrary solution to obtain such a solution. The case 2 solutions are those such that p divides XYZ. These are harder to rule out (see Borevich and Shafarevich - Number Theory, 378-381). If you get stuck on anything below, the proof we are outlining follows Milne, starting halfway down p.102.

1. First, use GP/Pari to find some regular and irregular primes.
To prove the theorem, we argue by contradiction, so assume such a solution exists:
2. Rule out $p = 3$ by working modulo 9. Assume from now on that $p \geq 5$.
3. Show that we may assume $p \nmid X - Y$ (we cannot have $x \equiv y \equiv -z \mod p$, so if $x \equiv y$ build a new solution by swapping $Y \mapsto -Z$, $Z \mapsto -Y$.)
4. Show
$$\prod_{\zeta \in \mu_p(\mathbb{C})} (X - \zeta Y) = Z^p.$$
5. Show the factors on the left are relatively prime (hint: for any ζ and ζ' distinct pth roots of unity, the ideal $(\zeta - \zeta') = (1 - \zeta'/\zeta) = (1 - \zeta'')$ for ζ'' a primitive pth root of unity, and thus is equal to the unique prime ideal dividing (p)).
6. Deduce that each ideal $(X - \zeta Y)$ must be of the form I^p for an ideal I. Using the assumption on the class group, show the ideal I is principal, so $X - \zeta Y = u\alpha^p$ for $u \in \mathcal{O}^\times$ and $\alpha \in \mathcal{O}$. Using exercise 4, show we can can rewrite $X - \zeta Y = \zeta^r v \alpha^p$ for $v = \overline{v}$ a unit.
7. Show that for any $\alpha \in \mathcal{O}$ there is an integer a such that $\alpha^p \equiv a \mod (p)$.
8. We thus have $X - \zeta Y = \zeta^r va \mod p$ for a an integer and $v = \overline{v}$. Show also that $X - \overline{\zeta} Y = \zeta^{-r} va \mod p$.
9. Deduce that $X + \zeta Y - \zeta^{2r} X - \zeta^{2r-1} Y \equiv 0 \mod p$.
10. Show that if $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are distinct then p divides X and Y (hint: this is where we use $p \geq 5$). Deduce a contradiction.

(11) Treat the remaining cases (where these four are not distinct).