35 Final Remarks

35.1 Galois Theory in Finite Fields

We've seen that when F is a number field (a finite extension of $\mathbb{Q}$), the Galois group $\text{Gal}(E/F)$ can be complicated. But $\mathbb{Q}$ is only one of the primary fields — we can also consider finite extensions of $\mathbb{F}_p$ for p prime (which are the other primary fields). Then our base field is $F = \mathbb{F}_q$ where $q = p^m$ for some m, and a finite extension of F is $E = \mathbb{F}_{q^n}$ for some n.

In this case, the answer is much simpler, and we've essentially seen it already:

Theorem 35.1
The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is always a Galois extension; and $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic and generated by the **Frobenius automorphism** $\text{Fr}_q : x \mapsto x^q$.

Proof. We've seen earlier that

$$(a+b)^q = a^q + b^q,$$

so Fr_q is compatible with the field operations; and it's also one-to-one. So $\text{Fr}_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a field automorphism. Its fixed points are exactly the set $\{x \mid x^q = x\} = \mathbb{F}_q$. So then we know $\text{Fr}_q \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

But we can also compute its order — we know $\text{Fr}_q^a : x \mapsto x^{q^a}$. For $a = n$, we have that $\text{Fr}_{q^n} = \text{Id}$ (since $x^{q^n} = x$ for all $x \in \mathbb{F}_{q^n}$). Meanwhile, if $1 \le a < n$, not all $x \in \mathbb{F}_{q^n}$ satisfy $x^{q^a} = x$. So then $\text{ord}(\text{Fr}_q) = n$. This means

$$\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \supset \mathbb{Z}/n\mathbb{Z}$$

(considering the cyclic group generated by Fr_q). But we have $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, so the Galois group cannot have more than n elements; so we must have $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n\mathbb{Z}$. □

Note 35.2
Properties of the Frobenius automorphism are useful when doing algebraic geometry in fields of positive characteristic. In order to count the number of solutions to a system of polynomial equations over $\mathbb{F}_q$, one first looks at solutions over its algebraic closure $F = \bigcup \mathbb{F}_{q^n}$ (a bigger field in which every polynomial has a root, similarly to $\mathbb{C}$). Then solutions in $(\mathbb{F}_q)^n$ are the fixed points of $\text{Fr}_q : (x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q)$. One uses intuition from a similar problem in topology, of counting the number of fixed points of an automorphism of some geometric shape X. (This relates to the Lipschitz Fixed Points Theorem and the Weil conjectures.)

35.2 Further Directions

Finally, we'll go over the topics that have been covered in this class, and where they can lead.

35.2.1 Representation Theory

The first topic we discussed is the representations of finite groups. The class **18.715** develops this topic.

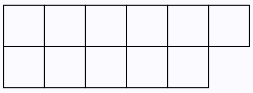
We've actually already seen the main general structural theorems about the representations of an *abstract* finite group; but one further direction is the classification and computation of the characters of irreducible representations for a *specific* group — in particular, S_n. We know the number of irreducible representations equals the number of conjugacy classes. But in this case, it's actually possible to index both by the same set — the set of partitions of n (ways to write $n = n_1 + \cdots + n_k$, where order doesn't matter). It turns out that irreducible representations are in bijection with partitions. Meanwhile, partitions are also in bijection with the cycle type of a permutation (which determines the conjugacy class) — in order to describe a conjugacy class, we're interested in the lengths of the cycles.

Example 35.3
The conjugacy class of $(12)(345)$ can be described by the partition $5 = 3 + 2$.

Partitions are usually depicted by Young diagrams, where the length of rows correspond to the summands. (These are also studied in classes on combinatorics.)

Example 35.4

The Young diagram



corresponds to the partition $11 = 6 + 5$.

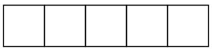
As an example of how this correspondence can be used, recall a problem we saw earlier:

Example 35.5

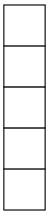
For which n is $\tau \otimes \text{sgn} = \tau$? (Here τ is the tautological representation of S_n, where elements of S_n act on the space with $x_1 + \cdots + x_n = 0$ by permuting coordinates.)

Earlier, we solved this directly by looking at the characters, but there's a nice way to solve it by looking at Young diagrams as well.

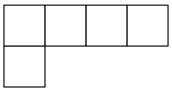
In this correspondence, the Young diagram



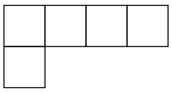
(corresponding to $n = n$) corresponds to the trivial representation, and the Young diagram



(corresponding to $n = 1 + 1 + \cdots + 1$) corresponds to sgn. Meanwhile, the Young diagram



(corresponding to $n = (n - 1) + 1$) corresponds to τ. More generally, $\rho \otimes \text{sgn}$ corresponds to the transpose of the diagram for ρ. So the fact that $\tau \otimes \text{sgn} = \tau$ exactly when $n = 3$ corresponds to the observation that the transpose of



(where we reflect it over the diagonal) is itself if and only if $n = 3$.

35.2.2 Compact Lie Groups

Another direction in which representation theory can lead is compact Lie groups:

Definition 35.6

A compact Lie group is a closed compact subgroup in $\text{GL}(n, \mathbb{C})$.

Example 35.7

One compact Lie group (which we've mentioned earlier) is $\text{SU}(2)$. Some other compact Lie groups include $\text{U}(n)$, $\text{SU}(n)$, $\text{SO}(n)$, and the *quaternionic unitary groups* $\text{Sp}(n)$ (which we haven't seen before).

It turns out that there's a classification of all such groups, along with some exceptional ones — G_2, F_4, E_6, E_7, and E_8. The largest exceptional group, E_8, has dimension 248. This can be studied further in **18.745** and **18.755**.

For each such group, there's also a classification of its irreducible representations.

Fact 35.8

The irreducible representations of $\mathrm{U}(n)$ are indexed by sequences of n integers $d_1 \geq \cdots \geq d_n$.

Example 35.9

Irreducible representations of $\mathrm{SU}(2)$ are indexed by one nonnegative integer n. To n, we assign the action on the space V_n of homogeneous polynomials of degree n in two variables (so V_n has a basis consisting of x^n, $x^{n-1}y$, $\ldots$, y^n, and has dimension $n+1$).

This connects to a more familiar situation — recall that $\mathrm{SU}(2)/\{\pm 1\} = \mathrm{SO}(3)$ (which is the group of rotations in 3-space). Then V_n for even n comes from a representation of $\mathrm{SO}(3)$.

This has an application to the spectrum of a hydrogen atom and the structure of the periodic table. The rows of the table have lengths 2, 8, 8, 18, 18, 32, 32 — these are $2n^2$ for small n, and n^2 arises as $1+3+\cdots+(n-1)$, where the odd numbers come from the dimensions of irreducible representations of $\mathrm{SO}(3)$.

The connection comes from an optional problem set problem on greedy monsters — we had monsters at the vertices of a cube, each with some amount of gold; and at every minute, the gold of each monster is equally distributed among its neighbors. The question asked us to understand how this process behaves over a long time. This is a special case of the Laplace operator on a graph:

Definition 35.10

Given a graph with certain weights assigned to the vertices, the **Laplace operator** redistributes the weight of every vertex equally among its neighbors.

This is the discrete version of the Laplace operator, but there's also a continuous version — for functions on $\mathbb{R}^2$, take the differential operator

$$\Delta = \frac{d^2}{dx^2} + \frac{d^2}{dy^2}.$$

This measures the extent to which the function is not harmonic — it vanishes exactly on functions whose value at each point is the average of the values on a small circle around it. (This is a continuous analog of the greedy monsters case, where our operator vanishes when the weight of each point equals the average weight of its neighbors.)

For symmetric graphs (such as the cube, in the case of the greedy monsters), we can understand the eigenvalues and eigenvectors of the operator using representation theory (as we did in the optional problem). Meanwhile, for the Laplace operator of the sphere S^2, its eigenvalues can be analyzed using representation theory of $\mathrm{SO}(3)$; these eigenvalues then have connections to quantum physics.

Another important identity we saw was that

$$|G| = \sum d_i^2,$$

where the d_i are the dimensions of irreducible representations. This fact came from looking at the regular representation $\mathbb{C}[G]$, and decomposing it as

$$\mathbb{C}[G] = \bigoplus V_i^{d_i}.$$

But we have $V_i^{d_i} \cong \mathrm{End}(V_i)$, where we can think of $\mathrm{End}(V_i)$ as $\mathrm{Mat}_{d_i}(\mathbb{C})$ (this is because V_i is d_i-dimensional, so specifying an endomorphism (or linear operator) on V_i is the same as specifying the d_i images of the basis vectors). So we can write

$$\mathbb{C}[G] \cong \bigoplus \mathrm{End}(V_i).$$

This generalizes to compact groups — except that if looking at functions, a typical function can't be written as a *sum* of elements, but rather as an infinite series. So we instead have

$$C(G) = \widehat{\bigoplus \mathrm{End}(V_i)}.$$

Example 35.11
If $G = \mathrm{U}(1)$ (which is just $S^1 = \{z \mid |z| = 1\}$), then irreducible representations are indexed by integers. This turns into the theory of Fourier series, as mentioned earlier.

The generalization of this case is harmonic analysis, where functions on the group are written in terms of an infinite series. In fact, to understand the spectrum of the Laplacian on the sphere, we consider this decomposition for functions on SO(3).

But if we don't work with infinite series, and just consider $\bigoplus \mathrm{End}(V_i)$, then we arrive at the notion of an algebraic group — we have

$$\mathrm{MSpec}(\bigoplus \mathrm{End}(V_i)) = G_{\mathbb{C}},$$

where $G_{\mathbb{C}}$ is an algebraic group (for example, $\mathrm{GL}(n, \mathbb{C})$). This is studied in **18.737**.

Beyond the theory of representations of compact groups, one can also work with *non-compact* Lie groups (closed but not necessarily compact subgroups of $\mathrm{GL}(n, \mathbb{C})$), such as $\mathrm{SL}(n, \mathbb{R})$. Then most representations are infinite-dimensional. This is also studied in **18.755** and its continuations.

35.2.3 Factorization

We've seen a story about factorization in quadratic number fields. This is considered closer to number theory than abstract algebra — factorization in $\mathbb{Z}(\sqrt{d})$ generalizes to rings of algebraic integers in number fields. This is studied in number theory, by using the action of the Galois group. A typical question is to start with a prime ideal in a number field, and try to understand how it decomposes in a larger number field.

An example of this is quadratic reciprocity, a classical result in number theory (which is explained in **18.781**). Part of the theorem is the following:

Example 35.12
If p and q are primes with $p \equiv 1 \pmod 4$, then p is a square mod q if and only if q is a square mod p.

This is an important result with many proofs, including elementary ones. But there's also a proof that generalizes and connects well to algebraic number theory, and in fact it relates to ideas we've seen in class. The idea is to consider $\mathbb{Q}(\zeta_p)$, where $\zeta_p = \exp(2\pi i/p)$. As proved in class, this contains $\mathbb{Q}(\sqrt{\pm p})$. By analyzing the factorization of q in these two fields, and looking at it in two ways using the description of the Galois group, one can obtain this beautiful statement. In number theory, this is generalized to higher reciprocity laws.

35.2.4 Rings and Modules

In rings and modules, one of the main theorems we saw was the classification of finitely generated modules over a PID. The class **18.705** on commutative algebra develops this much further.

Commutative algebra is also closely related to algebraic geometry. For example, if we have a ring $R = \mathbb{C}[x_1, \dots, x_n]/I$, we can consider its maximal spectrum $\mathrm{MSpec}(R) \subset \mathbb{C}^n$.

Then for an R-module M and $x \in \mathrm{MSpec}(R)$, we get a $\mathbb{C}$-vector space — x corresponds to a maximal ideal $\mathfrak{m}_x$, and $R/\mathfrak{m}_x = \mathbb{C}$ (as we proved using Nullstelensatz). So $M/\mathfrak{m}_x M$ is a $\mathbb{C}$-vector space (which is finite-dimensional if M was finitely generated). This gives a family of vector spaces indexed by $x \in \mathrm{MSpec}(R)$. This idea is also studied in topology and differential geometry, namely vector bundles; and this analogy (connecting it to ideals in commutative algebra) is important.

35.2.5 Galois Theory

We saw a story relating groups to extensions; the key examples were extensions of number fields and of $\mathbb{C}(t)$ (the latter was just sketched, but it's still an important example).

Historically, at about the same time Galois worked on this, Abel was thinking about the same problem, but more in terms of geometry. Galois theory as presented here allows us to say that for a *specific* polynomial equation, there's no formula for the solution in radicals. On the other hand, Abel's work considered universal formulas, and showed that they relate to Riemann surfaces (which relate to complex analysis).

Resource: Algebra II Student Notes
Spring 2022
Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng