Math 250A Lecture 25 Notes

Daniel Raban

November 28, 2017

1 Hilbert's Theorem 90 and Galois Cohomology

1.1 Hilbert's theorem 90

We will begin by proving this oddly named[1] theorem we started last lecture.

Theorem 1.1 (Hilbert's theorem 90)**.** *Suppose L/K us cyclic. Then $N(a) = 1$ iff $a = b/\sigma b$ for some $b \in L^*$.*

Proof. If $a = a/\sigma b$, we leave it as an exercise to show that $N(a) = 1$.

We want to solve $a\sigma b = b$. Think of $a\sigma$ as a linear transformation on the vector space L; we want to find some $b \neq 0$ fixed by this linear transformation. Does $a\sigma$ have finite order? $(a\sigma)^2 = a\sigma a\sigma$, so it takes $b \mapsto a\sigma(a\sigma(b)) = a\sigma(a)\sigma^2(b)$. So $(a\sigma)^2 = a\sigma(a)\sigma^2$. We can continue this to get

$$(a\sigma)^n = \underbrace{a\sigma a\sigma^2 a \cdots \sigma^{n-1} a}_{N(a)=1} \underbrace{\sigma^n}_{=1} = 1.$$

A fixed vector of any G is given by $\sum_{g \in G} g(v)$. So the vector fixed by $(a\sigma)$ is given by $b = \sum i \in \mathbb{Z}(a\sigma)^i(\theta)$ for any $\theta \in L$. So b solves the problem, except we do not know that $b \neq 0$. What is the correct choice of theta? Note that this is

$$\begin{aligned} \theta + a\sigma(\theta) + (a\sigma)^2\theta + \cdots &= \theta + a\sigma\theta + a\sigma(a)\sigma^2(\theta) + a\sigma(a)\sigma^2(a)\sigma^3(\theta) \\ &= (a_0\sigma^0 + a_1\sigma^1 + a_2\sigma^2 + \cdots)(\theta) \end{aligned}$$

Use Artin's lemma to get that the σ_i are linearly independent. We can then find a θ so that the sum is 0.[2]

□

We will see later that this means that $H^{-1}(L^*) = 0$ for L/K cyclic. Here, $H^{-1}(L^*)$ is the *Tate cohomology group*.

[1] The name comes from Hilbert's "Zahlbericht" (number report) in 1897

[2] Professor Borcherds does not like the way Lang did this proof. Lang pulls out the second expression out of nowhere. Professor Borcherds says it seems like a "deus ex machina."

1.2 Applications of Hilbert's theorem 90

Example 1.1. Suppose K contains a primitive n-th root ζ of unity. Take $a = \zeta$. Then $N(a) = \zeta\zeta\cdots\zeta = 1$. So $a = b/\sigma b$ for some b. So $\sigma(b) = \zeta b$. This makes $\sigma(b^n) = b^n$, so $b^n \in K^*$. So $L = K(\sqrt[n]{*})$.

Example 1.2. Let's solve $x^3 + x + 1 = 0$. The discriminant is -31, which is not a square in $\mathbb{Q}$, so the Galois group of the splitting field of this polynomial over $\mathbb{Q}$ is S_3. This is a solvable group because we have $1 \subseteq \mathbb{Z}/3\mathbb{Z} \subseteq S_3$. This gives us the picture

$$\begin{tikzcd}
L \arrow[d, dash, "3"] & 1 \arrow[d, dash, "3"] \\
K \arrow[d, dash, "2"] & \mathbb{Z}/3\mathbb{Z} \arrow[d, dash, "2"] \\
\mathbb{Q}(\omega) & S_3
\end{tikzcd}$$

What is K? K is a subfield of L fixed by $\mathbb{Z}/3\mathbb{Z}$. S_3 acts on $\alpha_1, \alpha_2, \alpha_3$. Let σ be a generator of $\mathbb{Z}/3\mathbb{Z}$. Then σ maps $\alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1$. K is generated by some α, where α is fixed by σ, but the elements of S_3 are not in $\mathbb{Z}/3\mathbb{Z}$. Try $\alpha = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ (find some polynomial in $\alpha_1, \alpha_2, \alpha_3$ fixed by $\mathbb{Z}/3\mathbb{Z}$ but not S_3. Now

$$\alpha^2 = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2$$

is symmetric in α_i, so it is in the base field. It is the discriminant of $x^3 + x + 1$, which is -31. So $K = \mathbb{Q}(w, \sqrt{-31})$.

Next, we want to describe L in terms of K. L/K is a cyclic extension, so K contains cube roots of 1. So by Hilbert's theorem 90, $L = K(\sqrt[3]{*})$, where $*$ is an eigenvector of σ with eigenvalue equal to ω. Try $\alpha_1 + \omega^{-1}\sigma(\alpha_1) + \omega^{-1}\sigma^2(\alpha_1) = \alpha_1 + \omega^{-1}\alpha_2 + \omega^{-2}\alpha_3$. Call this y. Let $z = \alpha_1 + w\alpha_2 + w^2\alpha_3$. If we find $y, z, 0$, we can find $\alpha_1, \alpha_2, \alpha_3$ by linear algebra.

We know that $y^3, z^3 \in K$ and are fixe by σ.Expand these in polynomials in $\alpha_1, \alpha_2, \alpha_3$ to get that $y^3 + z^3 = -27$ and $y^3 b^3 = -27$. So we get that y^3 and z^3 are roots of $x^2 + 27z - 27 = 0$. So $y^3, z^3 = 27/2 \pm 3\sqrt{3}i/2\sqrt{-31}$, which means that y, z are given by $y = -3.04\ldots$ and $z = 0.99\ldots$. So $\alpha_1 = (y + z)/3 \approx -0.68\ldots$[3]

Example 1.3. Let's solve degree 4 equations $x^4 + bx^2 + cd + d$ by radicals. We will provide a sketch. Look at the Galois group S_4, which is solvable because $1 \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq A_4 \subseteq S_4$.

[3] Why do we put these approximate values? It's so you can check the answer for yourself!

We will have

$$\begin{array}{c} M \\ \Big| \scriptstyle 4 \\ L \\ \Big| \scriptstyle 3 \\ K \\ \Big| \scriptstyle 2 \\ \mathbb{Q}(\omega, i) \end{array} \qquad \qquad \begin{array}{c} 1 \\ \Big| \scriptstyle 4 \\ (\mathbb{Z}/2\mathbb{Z})^2 \\ \Big| \scriptstyle 3 \\ A_4 \\ \Big| \scriptstyle 2 \\ S_4 \end{array}$$

To get to K from $\mathbb{Q}(\omega, i)$, we will adjoin a square root. Going up the diagram, we will then adjoin a cube root and then another square root.

Suppose the roots are $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Note that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. What is L? It is generated by things fixed under $(\mathbb{Z}/2\mathbb{Z})^2$. We wan to find a polynomial fixed by $(\mathbb{Z}/2\mathbb{Z})^2 \subseteq \S_4$. Try $y_1 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2/4 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$. It has conjugates

$$y_2 = (\alpha_1 + \alpha_3 - \alpha_2 - \alpha_4)^2/4$$

$$y_3 = (\alpha_1 + \alpha_4 4 - \alpha_2 - \alpha_3)^2/4$$

If we find $y_1, y_2, y_3,$, we can find $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ using some algebra.

y_1, y_2, y_3 generate a degree 6 extension of $\mathbb{Q}(\omega, i)$. The Galois group is $S_3 = S_4/(\mathbb{Z}/2\mathbb{Z})^2$. So y_1, y_2, y_3 are the roots of some cubic over $\mathbb{Q}$. In fact, there are the roots of $y^3 - 2by^2 + (b^2 - d)y_x^2 = 0$, which you can obtain via some messy algebra.[4] We can solve this cubic to find y_1, y_2, y_3 and use those to find the α_i.

1.3 Galois cohomology

1.3.1 Exact sequences

No one ever understands Galois cohomology the first time the encounter it.[5]

Suppose G is a group acting on some module M. Look at

1. M^G, the subset of things fixed by G (the invariants of G on M).

2. $M_G = M / \{m - gm : m \in M, g \in G\}$.

[4] Mathematicians tried to find this for degree 5, but it turns out to be a degree 6 polynomial, which is even worse than what you started with. The underlying fact driving this occurrence is that S_5 is not solvable.

[5] Professor Borcherds says that no one ever understands Galois cohomology the first time they encounter it. He even referred to this section as a "futile attempt" to explain it.

The former of these is the largest submodule of M where G acts trivially, and the latter is the largest quotient of M where G acts trivially.

Suppose that $0 \to A \to B \to C \to 0$ is an exact sequence. Act on it by G. Is this exact? No, we get

$$0 \to A^G \to B^G \to C^G \cancel{\to 0}.$$

Similarly, we get that

$$\cancel{0 \to} A_G \to B_G \to C_G \to 0.$$

Example 1.4. Take $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$. with $G = \mathbb{Z}/2\mathbb{Z}$ acting as -1 on $\mathbb{Z}$. We get

$$0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2|Z \to 0.$$

Note that $M^G = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$, where $\mathbb{Z}G$ is the group ring of G and $\mathrm{Hom}_{\mathbb{Z}G}$ is the homomorphisms preserving the action of G. So M is a module over $\mathbb{Z}G$. $\mathbb{Z}$ is a module over $\mathbb{Z}G$ iwth elements of G acting trivially ($g \cdot n = n$).

We had earlier in the course that $\mathrm{Hom}(*, *)$ does not preserve exactness, but the failure was controlled by "Ext." Similarly,

$$M_G = \mathbb{Z} \otimes_{\mathbb{Z}G} M.$$

The tensor product does not preserve exactness, but the failure is controlled by "Tor." Put $H^0(G, M) = M^G$. The zeroth cohomology is $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$. Put $H^i(G, M) = \mathrm{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, M)$.

A long exact sequence of Ext gives us that if

$$0 \to A \to B \to C \to 0$$

is exact, then so is

$$0 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to H^1(B) \to H^1(C) \to H^2(A) \to cdots$$

Similarly, put $H_0(G, M) = M_G$ and $H_i(G, M) = \mathrm{Tor}_i^{\mathbb{Z}G}(\mathbb{Z}, M)$. We get

$$\cdots \to H_1(C) \to H_0(A) \to H_0(B) \to H_0(C) \to 0$$

So H^1 and H_1 control the lack of exactness of M^G and M_G.

1.3.2 Lang's definition of cohomology

How does this relate to Lang's definition? Lang defines the first cohomology group as follows:

Definition 1.1. A *crossed homomorphism* is a map $G \to M$ sending $\sigma \mapsto a_\sigma$ with $a_{\sigma\tau} = a_\sigma + \sigma a_\tau$.

This is a homomorphism from $G \to M$ except if G acts trivially on M, then this is just $\mathrm{Hom}(G, M)$ as groups.

Definition 1.2. A *principal crossed homomorphism* is a crossed homomorphism such that $a_\sigma = b/\sigma b$ for some fixed b.

Lang defines the first cohomology group as

$$H^1(G, M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}}.$$

1.4 Hilbert's theorem 90 for all Galois extensions

Theorem 1.2 (Hilbert's theorem 90)**.** *Let L/K is a Galois extension with Galois group G. Then $H^1(G, L^*) = 0$.*

Proof. We are given $a_\sigma \in L^*$ with $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ (multiply, not add, since we are dealing with L^*, which is a multiplicative group). We want to find b with $a_\sigma = b/\sigma b$ for all σ. What is a crossed homomorphism? Look at $\sigma \mapsto a_\sigma \sigma$. This is a linear map $L \to L$, so $\sigma\tau \mapsto a_{\sigma\tau}\sigma\tau = a_\sigma \sigma a_\tau \tau = (a_\sigma \sigma)(a_\tau \tau)$. So this map is a homomorphism $G\ to\, \mathrm{End}(L)$. We will continue the proof next class. □