Hilbert's theorem 90

Seewoo Lee

February 15, 2022

In this note, we introduce Hilbert's theorem 90 and its applications.

1 Hilbert's theorem 90

Basically, Hilbert's theorem 90 is a vanishing theorem of some first Galois cohomology. Let E/F be a (finite) Galois extension. We can naturally view $E^\times$ as a $G = \mathrm{Gal}(E/F)$-module. With the G-module structure, Hilbert's theorem 90 claims that first group cohomology of G with coefficient $E^\times$ vanishes.

Theorem 1 (Hilbert)**.** *Let E/F be a Galois extension with a Galois group G. Then $\mathrm{H}^1(G, E^\times) = 0$.*

Proof. We need a following lemma:

Lemma 1. *Let E be a field and $\sigma_1, \dots, \sigma_n$ be a distinct automorphisms of E. Then they are E-linearly independent.*

Proof. Assume that they are not linearly independent. Let r be a number of nonzero coefficients among c_i's and assume that r is minimal among such r's. Also, we may assume that $c_1, \dots, c_r \neq 0$ and $c_{r+1} = \cdots = c_n = 0$. Then $r > 1$ since $c_1\sigma_1 = 0$ implies $c_1 = c_1\sigma_1(1) = 0$. Now choose $a \in E$ such that $\sigma_1(a) \neq \sigma_r(a)$. From

$$\begin{aligned} c_1\sigma_1(ax) + c_2\sigma_2(ax) + \cdots + c_r\sigma_r(ax) &= 0 \\ c_1\sigma_r(a)\sigma_1(x) + c_2\sigma_r(a)\sigma_2(x) + \cdots + c_r\sigma_r(a)\sigma_r(x) &= 0 \end{aligned}$$

we have

$$c_1(\sigma_1(a) - \sigma_r(a))\sigma_1(x) + \cdots + c_{r-1}(\sigma_{r-1}(a) - \sigma_r(a))\sigma_{r-1}(x) = 0.$$

By the way, we have $c_1(\sigma_1(a) - \sigma_r(a)) \neq 0$, and this contradicts to the minimality of r. □

We have to show that if $\alpha : G \to E^\times$ is a 1-cocycle, then it is a 1-coboundary, i.e. $\alpha = d\beta \Leftrightarrow \alpha_\sigma = \sigma(\beta)/\beta$ for any $\sigma \in G$. Note that α is a 1-cocycle if and only if $\alpha_{\sigma\tau} = \alpha_\sigma\sigma(\alpha_\tau)$ for all $\sigma, \tau \in G$. For given 1-cocycle α, consider the map

$$\sum_{\sigma \in G} \alpha_\sigma \sigma : E \to E.$$

By the previous lemma, the above map is nonzero and we can find $\theta \in E$ such that $\gamma := \sum_{\sigma \in G} \alpha_\sigma \sigma(\theta) \neq 0$. Then we have

$$\sigma\gamma = \sum_{\sigma \in G} \sigma(\alpha_\tau)\sigma\tau(\theta) = \sum_{\tau \in G} \alpha_\sigma^{-1}\alpha_{\sigma\tau}\sigma\tau(\theta) = \alpha_\sigma^{-1} \sum_{\tau \in G} \alpha_{\sigma\tau}\sigma\tau(\theta) = \alpha_\sigma^{-1}\gamma$$

which implies that $\alpha_\sigma = \sigma(\beta)/\beta$ for $\beta = \gamma^{-1}$. □

This is a *modern* version of Hilbert's theorem 90. The original version is about when E/F is a cyclic extension.

Corollary 1. *Let E/F be a finite cyclic extension and let σ be a generator of the Galois group $G = \mathrm{Gal}(E/F)$. For $\alpha \in E$, if $\mathrm{N}_{E/F}(\alpha) = 1$, then $\alpha = \beta/\sigma(\beta)$ for some $\beta \in E$.*

Proof. Let $n = [E : F]$. $\mathrm{N}_{E/F}(\alpha) = 1$ is equivalent to $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$. From this assumption, we can define a 1-cocycle $\alpha : G \to E^\times$ such that $\alpha_\sigma = \alpha$. Then Hilbert's theorem 90 implies that α is a 1-coboundary, so we can find β such that $\alpha = \alpha_\sigma = \beta/\sigma(\beta)$. □

This is somehow multiplicative version of Hilbert's theorem 90. There's also additive version for the trace map.

Theorem 2 (Hilbert's theorem 90, Additive form)**.** *Let E/F be a cyclic extension of degree n with Galois group G. Let $G = \langle\sigma\rangle$. Then for $\alpha \in E$, $\mathrm{Tr}_{E/F}(\alpha) = 0$ if and only if $\alpha = \beta - \sigma(\beta)$ for some $\alpha \in E$.*

Proof. By the lemma again, we can prove that there exists $\theta \in E$ such that

$$\mathrm{Tr}_{E/F}(\theta) = \theta + \sigma(\theta) + \sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta) \neq 0.$$

Now put

$$\beta := \frac{1}{\mathrm{Tr}_{E/F}(\theta)}(\alpha\sigma(\theta)+(\alpha+\sigma(\alpha))\sigma^2(\theta)+\cdots+(\alpha+\sigma(\alpha)+\cdots+\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta))$$

then one can check $\alpha = \beta - \sigma(\beta)$ holds. □

More generally, we have $\mathrm{H}^r(G, E) = 0$ for any finite Galois extension E/F, by using the normal basis theorem and a vanishing property of cohomology of induced modules.

2 Pythagorean triples

Using Hilbert's theorem 90, we can find all Pythagorean triples, i.e. rational points on the circle $x^2 + y^2 = 1$.

Corollary 2. *Let a, b be rational numbers s.t. $a^2 + b^2 = 1$. Then there exists $c, d \in \mathbb{Z}$ s.t.*

$$(a, b) = \left(\frac{c^2 - d^2}{c^2 + d^2}, \frac{2cd}{c^2 + d^2} \right).$$

In other words, every rational point on the circle $x^2 + y^2 = 1$ has above form.

Proof. This directly follows from Hilbert's theorem 90 by applying to the extension $\mathbb{Q}(i)/\mathbb{Q}$. In fact, if $a^2 + b^2 = 1$, then $\alpha = a + bi \in \mathbb{Q}(i)$ has a norm 1, so there exists $c + di \in \mathbb{Q}(i)$ s.t.

$$\alpha = a + bi = \frac{c + di}{\sigma(c + di)} = \frac{c + di}{c - di} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2} i$$

and we obtain the theorem by multiplying common denominator of c and d. (Here $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ is the nontrivial element in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.) □

More generally, by considering the extension $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ for square-free integer $D > 0$, we can prove the following:

Corollary 3. *Let a, b be rational numbers s.t. $a^2 + Db^2 = 1$. Then there exists $c, d \in \mathbb{Z}$ s.t.*

$$(a, b) = \left(\frac{c^2 - Dd^2}{c^2 + Dd^2}, \frac{2cd}{c^2 + Dd^2} \right).$$

3 Kummer extension

Using the Hilbert's theorem 90, we can prove that any degree n cyclic extension can be obtained by adjoining certain n-th root of element, if the base field contains a primitive n-th root of unity.

Theorem 3. *Let F be a field and let $n \geq 1$ be a natural number with $(\mathrm{char}\, p, n) = 1$. Assume that F contains a primitive n-th root of unity, ζ_n. If E/F is a cyclic extension of degree n, then there exists $a \in F$ s.t. $E = F(\sqrt[n]{a})$.*

Proof. Let E/F be a cyclic extension of degree n and let $G = \mathrm{Gal}(E/F) = \langle \sigma \rangle$. Since $\mathrm{N}_{E/F}(\zeta_n^{-1}) = (\zeta_n^{-1})^n = 1$, by Hilbert's theorem 90, there exists $\alpha \in E^\times$ s.t. $\zeta_n^{-1} = \alpha/\sigma(\alpha) \Leftrightarrow \sigma(\alpha) = \zeta_n \alpha$. Then $\sigma^j(\alpha) = \zeta_n^j \alpha$ for any $0 \leq j \leq n - 1$, so α has n distinct conjugates and $[F(\alpha) : F] \geq n$. However, from $[E : F] = n$ and $F(\alpha) \subseteq E$, we have $E = F(\alpha)$. Moreover, $\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta_n^n \alpha^n = \alpha^n$, so $\alpha^n \in F$ and $E = F(\sqrt[n]{a})$ if we put $a = \alpha^n$. □

Kummer theory studies about such kind of extension. It states that any abelian extension of F of exponent dividing n is formed by extraction of roots of elements in F. Moreover, there exists a one-to-one correspondence abelian extensions of F of exponent n and subgroups of $F^\times/(F^\times)^n$.

4 Artin-Schreier extension

Using the additive form of Hilbert's theorem 90, we can prove that degree p extension of a characteristic p field can be obtained by adjoining a root of certain polynomial. This can be considered additive analogue of Kummer extension.

Theorem 4 (Artin-Schreier extension)**.** *Let F be a field of characteristic $p > 0$.*

1. *For any $a \in F$, the polynomial $x^p - x - a \in F[x]$ is completely reducible (every root of the polynomial is in F) or irreducible.*

2. *Conversely, if E/F is a cyclic extension of degree p, E is a splitting field of $x^p - x - a$ for some $a \in E$.*

Proof. 1. First, we can observe that if α is a root of the polynomial $f(x) = x^p - x - a$, then $\alpha + j$ is also root of the polynomial for any $0 \leq j \leq p-1$, since $(\alpha + j)^p - (\alpha + j) - a = \alpha^p - j^p - \alpha - j - a = \alpha^p - \alpha - a = 0$. Hence if $f(x)$ has a root in F, then every root of $f(x)$ is in F.

Now assume that $f(x)$ doesn't have a root in F. We claim that $f(x)$ is irreducible over F. Suppose that $f(x)$ is not irreducible, so that $f(x) = g(x)h(x)$ for some non-constant polynomials $g(x), h(x) \in F[x]$. If $\alpha \in \overline{F}$ is a root of $f(x)$, then as we mentioned above, $\alpha + j$ is a root for any $0 \leq j \leq p-1$. Thus $f(x) = \prod_{0 \leq j \leq p-1}(x - \alpha - j)$ and we have

$$g(x) = \prod_{j \in S}(x - \alpha - j), \quad h(x) = \prod_{j \notin S}(x - \alpha - j)$$

for some subset $S \subsetneq \{0, 1, \ldots, p-1\}$. If $d = |S|$, then the $(d-1)$-th coefficient of $g(x)$ is $-\sum_{j \in S}(\alpha + j) = -d\alpha - \sum_{j \in S} j \in F$, which implies $d\alpha \in F$. Since $0 < d < p$, we have $\alpha \in F$, which gives a contradiction. Hence $f(x)$ is irreducible over F.

2. Let E/F be a cyclic extension of degree p and let $G = \mathrm{Gal}(E/F) = \langle \sigma \rangle$. Since $\mathrm{Tr}_{E/F}(-1) = -p = 0$, by additive form of Hilbert's theorem 90, there exists $\alpha \in E$ s.t. $\alpha - \sigma(\alpha) = -1$, i.e. $\sigma(\alpha) = \alpha + 1$. Then $\sigma^j(\alpha) = \alpha + j$ for all $0 \leq j \leq p-1$, so α has p distinct conjugates and $[F(\alpha) : F] \geq p$. However, from $[E : F] = p$ and $F(\alpha) = E$, this gives $E = F(\alpha)$. Now we have

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha,$$

so $\alpha^p - \alpha \in F$ and α is a root of the polynomial $f(x) = x^p - x - a \in F[x]$, where $a = \alpha^p - \alpha$. □

In general, it is hard to find an irreducible polynomial over a finite field of given degree. However, the above theorem shows that for any prime p, the polynomial $x^p - x - 1$ is irreducible polynomial over $\mathbb{F}_p$.

5 Function fields

We can obtain the following interesting theorem for rational functions:

Theorem 5. *Let $f(x) \in \mathbb{C}(x)$ be a rational function which satisfies*

$$f(x)f(\zeta x)f(\zeta^2 x)\cdots f(\zeta^{n-1}x) = 1$$

for $\zeta = \zeta_n = e^{2\pi i/n}$, n-th root of unity. Then there exists $g(x) \in \mathbb{C}(x)$ s.t.

$$f(x) = \frac{g(x)}{g(\zeta x)}.$$

For example, $f(x) = \zeta$ clearly satisfies the condition, and we have $\zeta = g(x)/g(\zeta x)$ for $g(x) = 1/x$.

Proof. Actually, this is a direct consequence of Hilbert's theorem 90. Let $E = \mathbb{C}(x)$ and $F = \mathbb{C}(x^n)$ be a subfield. Then E/F is a Galois extension since E is a splitting field of the polynomial $y^n - x^n \in F[y] = \mathbb{C}(x^n)[y]$. It's Galois group is $G = \mathrm{Gal}(E/F) \simeq \mathbb{Z}/n\mathbb{Z}$, where the generator of the group is given by $\sigma : E \to E$, $\sigma(f(x)) = f(\zeta x)$.

Now the condition on $f(x)$ is equivalent to $\mathrm{N}_{E/F} f(x) = 1$. So by Hilbert's theorem 90, there exists $g(x) \in E$ s.t. $f(x) = g(x)/\sigma(g(x)) = g(x)/g(\zeta x)$. □

As one can see in the proof, the theorem also holds if we replace $\mathbb{C}$ by any field k with $(\mathrm{char}\, k, n) = 1$.