The Kummer Pairing

Alexander J. Barrios
Purdue University

12 September 2013

Preliminaries

Theorem 1 (Artin)**.** *Let $\psi_1, \psi_2, \ldots, \psi_n$ be distinct group homomorphisms from a group G into K^*, where K is a field. Then the group homomorphisms are linearly independent over K.*

Theorem 2 (Hilbert's Theorem 90)**.** *Let E/F be a cyclic extension of degree n with $G = \mathrm{Gal}\,(E/F) = \langle \sigma \rangle$. Then*

(a) for $\beta \in E$, $\mathrm{N}(\beta) = 1$ if and only if there exist $\alpha \in E^*$ such that $\beta = \alpha/\sigma(\alpha)$

(b) for $\beta \in E$, $\mathrm{Tr}(\beta) = 0$ if and only if there exist $a \in E$ such that $\beta = \alpha - \sigma(\alpha)$.

Proof. (a) ($\Longleftarrow$) Suppose $\beta = \frac{\alpha}{\sigma(\alpha)}$. Then

$$\mathrm{N}(\beta) = \frac{\mathrm{N}(a)}{\mathrm{N}(\sigma(\alpha))} = 1$$

since $\mathrm{N}(\alpha) = \mathrm{N}(\sigma(\alpha))$.

($\Longrightarrow$) Suppose that $\mathrm{N}(\beta) = 1$. Since $\mathrm{Id}_{K^*},\ \beta\sigma, \beta\sigma(\beta)\,\sigma^2, \ldots, \prod_{j=1}^{n-2} \sigma^j(\beta)\,\sigma^{n-1}$ are all distinct group homomorphisms from K^* to K^*, we have that

$$\chi = \mathrm{Id}_{K^*} + \beta\sigma + \beta\sigma(\beta)\,\sigma^2 + \cdots + \prod_{j=0}^{n-2} \sigma^j(\beta)\,\sigma^{n-1}$$

is a map which is not identically 0 by Artin's Theorem. So there exist a nonzero $\theta \in K^*$ such that $\alpha = \chi(\theta) \neq 0$. Now consider,

$$\begin{aligned}\sigma(\alpha) = \sigma(\chi(\theta)) &= \sigma(\theta) + \sigma(\beta)\,\sigma^2(\theta) + \sigma(\beta)\,\sigma^2(\beta)\,\sigma^3 + \cdots + \prod_{j=0}^{n-2} \sigma^{j+1}(\beta)\,\sigma^n(\theta) \\ &= \sigma(\theta) + \sigma(\beta)\,\sigma^2(\theta) + \sigma(\beta)\,\sigma^2(\beta)\,\sigma^3 + \cdots + \prod_{j=1}^{n-2} \sigma^j(\beta)\,\sigma^{n-1}(\theta) + \prod_{j=1}^{n-1} \sigma^j(\beta)\,\theta.\end{aligned}$$

Now consider,

$$\begin{aligned}
\beta\sigma(\alpha) &= \beta\sigma(\theta) + \beta\sigma(\beta)\,\sigma^2(\theta) + \beta\sigma(\beta)\,\sigma^2(\beta)\,\sigma^3 + \cdots + \beta\prod_{j=1}^{n-2}\sigma^j(\beta)\,\sigma^{n-1}(\theta) + \beta\prod_{j=1}^{n-1}\sigma^j(\beta)\,\theta \\
&= \beta\sigma(\theta) + \beta\sigma(\beta)\,\sigma^2(\theta) + \beta\sigma(\beta)\,\sigma^2(\beta)\,\sigma^3 + \cdots + \prod_{j=0}^{n-2}\sigma^j(\beta)\,\sigma^{n-1}(\theta) + \mathrm{N}(\beta)\,\theta \\
&= \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\,\sigma^2(\theta) + \beta\sigma(\beta)\,\sigma^2(\beta)\,\sigma^3 + \cdots + \prod_{j=0}^{n-2}\sigma^j(\beta)\,\sigma^{n-1}(\theta) \\
&= \alpha
\end{aligned}$$

and so $\beta = \frac{\alpha}{\sigma(\alpha)}$.

(b) ($\Longleftarrow$) Suppose $\beta = \alpha - \sigma(\alpha)$. Then

$$\begin{aligned}
\mathrm{Tr}(\beta) &= \mathrm{Tr}(\alpha - \sigma(\alpha)) \\
&= \mathrm{Tr}(\alpha)\,p - \mathrm{Tr}(\sigma(\alpha)) \\
&= 0
\end{aligned}$$

since $\mathrm{Tr}(\alpha)\,p = \mathrm{Tr}(\sigma(\alpha))$.

($\Longrightarrow$) Now suppose $\mathrm{Tr}(\beta) = 0$. By Artin's Theorem we have that

$$\chi = \beta\sigma + (\beta + \sigma(\beta))\,\sigma^2 + \cdots + \sum_{j=0}^{n-2}\sigma^j(\beta)\,\sigma^{n-1}$$

is not identically zero on K^*. So there exist $\theta \in K^*$ with $\mathrm{Tr}(\theta) \neq 0$ and $\chi(\theta) \neq 0$. Set $\alpha = \frac{1}{\mathrm{Tr}(\theta)}\chi(\theta)$. Then

$$\begin{aligned}
\sigma(\alpha) &= \frac{1}{\sigma(\mathrm{Tr}(\theta))}\left(\sigma(\beta)\,\sigma(\theta) + \left(\sigma(\beta) + \sigma^2(\beta)\right)\sigma^2(\theta) + \cdots + \sum_{j=0}^{n-2}\sigma^{j+1}(\beta)\,\sigma^n(\theta)\right) \\
&= \frac{1}{\mathrm{Tr}(\theta)}\left(\sigma(\beta)\,\sigma(\theta) + \left(\sigma(\beta) + \sigma^2(\beta)\right)\sigma^2(\theta) + \cdots + \sum_{j=1}^{n-1}\sigma^j(\beta)\,\theta\right).
\end{aligned}$$

So we get that

$$\begin{aligned}
\alpha - \sigma(\alpha) &= \frac{1}{\mathrm{Tr}(\theta)}\left(\beta\sigma(\theta) + (\beta + \sigma(\beta))\,\sigma^2(\theta) + \cdots + \sum_{j=0}^{n-2}\sigma^j(\beta)\,\sigma^{n-1}(\theta)\right) \\
&\quad - \frac{1}{\mathrm{Tr}(\theta)}\left(\sigma(\beta)\,\sigma(\theta) + \left(\sigma(\beta) + \sigma^2(\beta)\right)\sigma^2(\theta) + \cdots + \sum_{j=1}^{n-1}\sigma^j(\beta)\,\sigma^{n-1}(\theta) + \sum_{j=1}^{n-1}\sigma^j(\beta)\,\theta\right) \\
&= \frac{1}{\mathrm{Tr}(\theta)}\left(\sigma(\theta)\,(\beta - \sigma(\beta)) + \sigma^2(\theta)\left(\beta - \sigma^2(\beta)\right) + \cdots + \sigma^{n-1}(\theta)\left(\beta - \sigma^{n-1}(\beta)\right) - \sum_{j=1}^{n-1}\sigma^j(\beta)\,\theta\right) \\
&= \frac{1}{\mathrm{Tr}(\theta)}\left(\beta\,\mathrm{Tr}(\theta)\right)
\end{aligned}$$

and so $\beta = \alpha - \sigma(\alpha)$. □

Remark Part (a) and (b) above are called the multiplicative form of Hilbert's 90^{th} and the additive form of Hilbert's 90^{th}, respectively.

Proposition 3. *Let F be a field and n be a natural number not dividing* $\operatorname{char} F = p$ *if $p > 0$. Suppose ζ_n is a primitive n^{th} root of unity lying in F.*

(a) If E/F is cyclic of degree n, then there exist $\alpha \in E$ such that $E = F(\alpha)$ and α satisfies $X^n - a = 0$ for some $a \in F$.

(b) If α is a root of $X^n - a$ where $a \in F$, then $F(\alpha)$ is cyclic over F of order d, where $d|n$ and $\alpha^d \in F$.

Proof. (a) Let ζ be a primitive n-th root of unity in F. Let $G = \operatorname{Gal}(E/F) = \langle\sigma\rangle$, since E/F is cyclic. Since $\mathrm{N}\left(\zeta^{-1}\right) = \left(\zeta^{-1}\right)^n = 1$, we have by Hilbert's 90^{th} Theorem that there exist $\alpha \in E^*$ such that $\zeta^{-1} = \frac{\alpha}{\sigma(\alpha)} \iff \sigma(\alpha) = \zeta\alpha$. Since $\zeta \in F$, we have that $\sigma(\zeta) = \zeta$ and so $\sigma^2(\alpha) = \sigma(\zeta)\,\sigma(\alpha) = \zeta^2\alpha$ and this in turn implies that for $j \in \{1, \ldots, n\}$, we have $\sigma^j(\alpha) = \sigma^j\alpha$. In particular, each $\zeta^j\alpha$ is a conjugate of α over F, and so $[F(\alpha) : F] \geq n$. Since $[E : F] = n$ and $F(\alpha) \subset K$, we conclude that $E = F(\alpha)$. Moreover, $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n$ and therefore α^n is fixed by σ, i.e., $\alpha^n \in F$. Let $a = \alpha^n$, then $X - a$ is a minimal polynomial for α over F.

(b) Conversely, let $a \in F$ and α be a root of $X^n - a$. Then each $\alpha\zeta^j$ for $j \in \{1, \ldots, n\}$ is also a root $X^n - a$. Therefore all roots lie in $F(\alpha)$ and hence $F(\alpha)/F$ is Galois. Let $G = \operatorname{Gal}(F(\alpha)/F)$. If $\sigma \in G$, then $\sigma(\alpha)$ is also a root of $X^n - a$. Thus $\sigma(\alpha) = \omega_\sigma\alpha$ where ω_σ is an n-th root of unity. In particular, the map $\sigma \longmapsto \omega_\sigma$ is an injective group homomorphism of G into μ_n. Since μ_n is cyclic, we have that G must by cyclic of order d where $d|n$. If $\langle\sigma\rangle = G$, then ω_σ is a primitive d-th root of unity and we get

$$\sigma\left(\alpha^d\right) = \sigma(\alpha)^d = (\omega_\sigma\alpha)^d = \alpha^d,$$

which implies that $\alpha^d \in F$, as claimed. □

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

(a) Let E/F be cyclic of order p. Then there exists $\alpha \in E$ such that $E = F(\alpha)$ and α satisfies $X^p - X - a = 0$ for some $a \in F$.

(b) Conversely, given $a \in F$, the polynomial $f(X) = X^p - X - a$ either has one root in F, in which case all its roots are in F, or it is irreducible. In this latter case, if α is a root then $F(\alpha)$ is cyclic of degree p over F.

Proof. (a) Suppose that E/F is cyclic of order p and let $G = \operatorname{Gal}(E/F) = \langle\sigma\rangle$. Since $\operatorname{Tr}(-1) = p\,(-1)$, we have by Hilbert's 90^{th} Theorem that there exist $\alpha \in E$ so that $\sigma(\alpha) = \alpha + 1$. In particular, $\sigma^2(\alpha) = \sigma(\alpha) + 1 = \alpha + 2$ and in general we have $\sigma^j(\alpha) = \alpha + j$ for $j \in \{1, \ldots p\}$. Therefore α has p distinct conjugates and so $[F(\alpha) : F] \geq p$. But by assumption $[E : F] = p$ which forces $E = F(\alpha)$ since $F(\alpha) \subset E$. Note that

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

thus $\alpha^p - \alpha$ is fixed by G and hence $\alpha^p - \alpha \in F$. Now take $a = \alpha^p - \alpha$ and therefore α satisfies $X^p - X - a = 0$.

(b) Now let $a \in F$ and consider the polynomial $f(X) = X^p - X - a$. Suppose α is a root of $f(X)$. Then $\alpha + j$ for $j \in \{1, \ldots, p\}$ are also roots of $f(X)$ since

$$(\alpha + j)^p - (\alpha + j) - a = \alpha^p + j^p - \alpha - j - a = \alpha^p - \alpha - a = 0.$$

In particular, $f(X)$ has p distinct roots. If some root α lies in F, it follows that every root is in F. So suppose that no root α lies in F.

We claim that $f(X)$ is an irreducible polynomial. Suppose on the contrary that it is reducible over F, then $f(X) = g(X)\,h(X)$ for some $g(X), h(X) \in F[X]$ with their degrees being strictly less than p. If α is a root of f, then

$$f(X) = \prod_{j=0}^{p-1} (X - \alpha - j).$$

It follows that both f and g are products of certain distinct integers j. That is, there exist $I, J \subset \{0, \ldots, p-1\}$ such that $I \cap K = \varnothing$ and $I \cup J = \{0, \ldots, p-1\}$ and

$$g(X) = \prod_{i \in I} (X - \alpha - i) \text{ and } h(X) = \prod_{k \in K} (X - \alpha - k).$$

Let $d = \deg g$ and write $g(X) = \sum_{l=0}^{d} g_l X^l$. Then $g_{d-1} = \sum_{i \in I} -(\alpha + i)$ by the theory on symmetric polynomials. Since $|I| = d$, we have that $g_{d-1} = -d\alpha + m$ for some $m \in \mathbb{F}_p$. Since $d \neq 0$ and $g_{d-1} \in F$, it follows that $\alpha \in F$, which is a contradiction and therefore f is irreducible.

Moreover, each root of f then lies in $F(\alpha)$ and so $F(\alpha)/F$ is Galois. Let $G = \mathrm{Gal}(F(\alpha)/F)$. Then there exist $\sigma \in G$ such that $\sigma(\alpha) = \alpha + 1$. But this implies that $\sigma^j(\alpha) = \alpha + j$ for each $j \in \{0, \ldots, p-1\}$. Since each $\alpha + j$ is a distinct root of $f(X)$, we conclude that G is cyclic and it is generated by σ, as desired. □

Abelian Kummer Theory

Definition A group G is said to be **exponent** $m > 0$ if $\sigma^m = 1$ for each $\sigma \in G$.

Let μ_m denote the group of m-th roots of unity. Throughout this section we will assume that $m \nmid \mathrm{char}\, F = p$ if $p > 0$. We will also assume that $\mu_m \subset F$ and we denote by $\bar{F}$, a fixed algebraic closure of F. Set $F^{*m} = \{a^m \in F^* \mid a \in F\}$.

Let $a \in F^*$ and consider $F\left(a^{1/m}\right)$. This is well-defined since $\mu_m \subset F^*$ implies that for any $\alpha, \beta \in \bar{F}$ satisfying $\alpha^m = \beta^m = a$, $F(\alpha) = F(\beta)$. Now let B be a subgroup of F^* containing F^{*m}. We denote by $K_B = F\left(B^{1/m}\right)$ the compositum of all $F\left(a^{1/m}\right)$ as a ranges over B. In particular, if $B = F^{*m}$, then $K_B = F$.

Notation 5. *By $A \subset_G B$ we mean that A is a subgroup of B.*

Lemma 6. *Let F be a field, m a natural number prime to $\mathrm{char}\, F = p$ if $p > 0$, and suppose $\mu_m \subset F$. Let $B \subset_G F^*$ such that B contains F^{*m} and let $K_B = F\left(B^{1/m}\right)$. Then the extension K_B/F is Galois and $G = \mathrm{Gal}(K_B/F)$ is abelian and of exponent m.*

Proof. Let $a \in B$ and let α be a m-th root of a. Then $X^m - a \in F[X]$ splits into linear factors in K_B, and thus K_B is Galois over F since this holds for each $a \in B$. □

Definition If B is a subgroup of F^* containing F^{*m}, we call its associated field extension K_B/F a **Kummer m-extension.**

Definition Let $B \subset_G F^*$ such that $F^{*m} \subset B$. The **Kummer pairing** is defined as

$$\kappa : \mathrm{Gal}(K_B/F) \times B \longrightarrow \mu_m \text{ where } \kappa(\sigma, a) = \omega_\sigma = \frac{\sigma(\alpha)}{\alpha} \text{ where } \alpha^m = a.$$

Theorem 7. *Let F be a field, m a natural number prime to $\mathrm{char}\, F = p$ if $p > 0$, and suppose $\mu_m \subset F$. Let $B \subset_G F^*$ such that B contains F^{*m} and let $K_B = F\left(B^{1/m}\right)$. Then*

(a) The Kummer pairing κ is a well-defined bilinear map;

(b) The kernel on the left is 1;

(c) The kernel on the right is F^{*m}.

Moreover, the Kummer pairing induces a perfect bilinear pairing

$$\kappa : G \times B/F^{*m} \longrightarrow \mu_m.$$

Proof. (a) Let $\alpha^m = \beta^m = a$. Then there is some $\zeta \in \mu_m$ such that $\beta = \alpha\zeta$. It follows that

$$\frac{\sigma(\beta)}{\beta} = \frac{\sigma(\alpha\zeta)}{\alpha\zeta} = \frac{\zeta\sigma(\alpha)}{\zeta\alpha} = \frac{\sigma(\alpha)}{\alpha}$$

and so κ is independent of the m-th root of a.

Moreover, the $\sigma \longmapsto \kappa(\sigma, a)$ is a homomorphism for each $a \in B$, since for $\sigma, \tau \in G$, we have that

$$\kappa(\sigma\tau, a) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma(\zeta_\tau\alpha)}{\alpha} = \frac{\zeta_\sigma\zeta_\tau\alpha}{\alpha} = \frac{\zeta_\sigma\alpha}{\alpha}\frac{\zeta_\tau\alpha}{\alpha} = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\alpha)}{\alpha} = \kappa(\sigma, a)\,\kappa(\tau, a)$$

and $a \longmapsto \kappa(\sigma, a)$ is a homomorphism since $a, b \in B$ with $\alpha^m = a$ and $\beta^m = b$, we have

$$\kappa(\sigma, ab) = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma(\beta)}{\beta} = \kappa(\sigma, a)\,\kappa(\sigma, b)\,,$$

thus κ is bilinear.

(b) Let $\sigma \in G$ and suppose $\kappa(\sigma, a) = 1$ for each $a \in B$. Then for every generator α of K_B with $\alpha^m = a$ we have that $\frac{\sigma(\alpha)}{\alpha} = 1$, i.e., $\sigma(\alpha) = \alpha$. Hence σ induces the identity on K_B and we conclude that the kernel on the left is 1.

(c) Let $a \in B$ and suppose $\kappa(\sigma, a) = 1$ for each $\sigma \in G$. Consider the subfield $F\left(a^{1/m}\right)$ of K_B. If $a^{1/m}$ is not in F, then there exist an automorphism of $F\left(a^{1/m}\right)/F$ which is not the identity. Extending this automorphism to K_B, we have that its extension by construction is not 1, and therefore $\kappa(a, \sigma) \neq 1$ if $a^{1/m} \notin F$. If $a^{1/m} \in F$, then $\sigma\left(a^{1/m}\right) = a^{1/m}$ and so we conclude that the kernel on the right consists of F^{*m}. □

Theorem 8. *Let F be a field, m a natural number prime to* $\operatorname{char} F = p$ *if $p > 0$, and suppose $\mu_m \subset F$. Let $B \subset_G F^*$ such that B contains F^{*m} and let $K_B = F\left(B^{1/m}\right)$. Then*

(a) The map $B \longmapsto K_B$ gives a bijection of the set of subgroups of F^* containing F^{*m} and the abelian extensions of k of order m.

(b) The extension is K_B/F is finite if and only if $(B : F^{*m})$ is finite. Moreover, if this is the case we have that $B/F^{*m} \cong \operatorname{Hom}(G, \mu_m)$ and $[K_B : F] = (B : F^{*m})$.

Proof. (a) Let B_1, B_2 be subgroups of F^* that contain F^{*m}. If $B_1 \subset B_2$, then $F\left(B_1^{1/m}\right) \subset F\left(B_2^{1/m}\right)$. Conversely, assume that $F\left(B_1^{1/m}\right) \subset F\left(B_2^{1/m}\right)$. We claim that $B_1 \subset B_2$. Let $b \in B_1$. Then $F\left(b^{1/m}\right) \subset F\left(B_2^{1/m}\right)$ and it is a finite generated subextension of $F\left(B_2^{1/m}\right)$. WLOG, suppose B_2/F^{*m} is finitely generated and therefore finite. Let $B_3 = \langle B_2, b\rangle$. Then B_3 is a finitely generated subgroup of F^* and in particular, $K\left(B_2^{1/m}\right) = K\left(B_3^{1/m}\right)$.Moreover, $(B_2 : F^{*m}) = (B_3 : F^{*m})$ and so $B_2 = B_3$ which gives us that $B_1 \subset B_2$. We conclude that we have an injection of our set of groups B into the set of abelian extensions of F of exponent m.

Now suppose that E is an abelian extension of F of exponent m. Any finite subextension is a composite of cyclic extensions of exponent m because any finite abelian group is a product of cyclic groups. In particular, it has only a finite number of intermediate fields. But we have seen that every cyclic extension can be obtained by adjoining a family of m-th roots of unity, say $\{b_j\}_{j\in J}$ with each $b_j \in F^*$. Let $B = \left\langle \{b_j\}_{j\in J}, F^{*m} \right\rangle$. If $b' = ba^m$ with $a, b \in F$, then $F\left(b^{1/m}\right) = F\left(b'^{1/m}\right)$ and so $F\left(B^{1/m}\right) = E$. □

Example Let E be the splitting field of $X^3 - a$ with $a \notin \mathbb{Q}^{*3}$. Then $\zeta_3, a^{1/3} \in E$. Let $F = \mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive 3-rd root of unity. We have that $F \subset_F E$. Note that L/F is Galois with group Z_3, and therefore it is abelian of exponent 3, therefore it is a Kummer 3-extension.

Example As an example consider $E = \mathbb{Q}(\zeta_7)$ where ζ_7 is a primitive 7-th root of unity. Let $F = \mathbb{Q}(2\operatorname{Re}\zeta_7)$. One can show $2\operatorname{Re}\zeta_7$ has minimal polynomial

$$m_F(x) = x^3 + x^2 - 2x - 1$$

and using Cardano's formula one can attain an exact value for $2\operatorname{Re}\zeta_7$. Moreover, $[F:\mathbb{Q}] = 3$ and $F/\mathbb{Q}$ is Galois since $m_F(x)$ splits into linear factors over F. That is, F is abelian of exponent 3. However $\mathbb{Q}(2\operatorname{Re}\zeta_7) \neq \mathbb{Q}\left(a^{1/3}\right)$ for any $a \in \mathbb{Q}$. This follows since if $\mathbb{Q}(2\operatorname{Re}\zeta_7) = \mathbb{Q}\left(a^{1/3}\right)$ for some $a \in \mathbb{Q}$, then $X^3 - a$ must split into linear factors over $\mathbb{Q}(2\operatorname{Re}\zeta_7)$. This in turn implies that $\zeta_3 \in \mathbb{Q}(2\operatorname{Re}\zeta_7)$, which implies that $\mathbb{Q}(2\operatorname{Re}\zeta_7) \not\subset \mathbb{R}$, a contradiction. This shows why it is essential that we make the assumption that the field contain the m-th roots of unity.

We now extend the theory to abelian extensions of exponent p equal to the characteristic of F. We will only prove the results for extensions of exponent p. However, the case of exponent p^n for $n > 1$ is due to Ernst Witt

Let F be a field of characteristic p. Let $\mathcal{P} : F \to F$ by $\mathcal{P}(a) = a^p - a$ for $a \in F$. Note that $\mathcal{P}$ is an additive homomorphism. In what follows, $\mathcal{P}(F) := F^p$ will be the analogue of F^{*m} above. For $a \in F$, we set $\mathcal{P}^{-1}(a)$ to be a root of the polynomial $X^p - X - a$. Let B be an additive subgroup of F containing F^p. We define $K_B = F\left(\mathcal{P}^{-1}B\right)$ to be the field obtained by adjoining $\mathcal{P}^{-1}(a)$ to F for each $a \in B$. Then we have results analogous to the above:

Let F be a field of characteristic p

Lemma 9. *Let F be a field of characteristic p. Let $B \subset_G F$ such that B contains F^p and let $K_B = F\left(\mathcal{P}^{-1}B\right)$. Then the extension K_B/F is Galois and $G = \operatorname{Gal}(K_B/F)$ is abelian and of exponent p.*

Definition If B is a subgroup of F^* containing F^p, we call its associated field extension K_B/F a **Kummer p-extension.**

Definition Let $B \subset_G F$ such that $F^p \subset B$. The **(additive) Kummer pairing** is defined as

$$\kappa : G \times B \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ where } \kappa_+(\sigma, a) = \sigma(\alpha) - \alpha \text{ where } \mathcal{P}(\alpha) = a.$$

Theorem 10. *Let F be a field of characteristic p. Let $B \subset_G F$ such that B contains F^p and let $K_B = F\left(\mathcal{P}^{-1}B\right)$. Then*

(a) The Kummer pairing κ_+ is a well-defined bilinear map;

(b) The kernel on the left is 1;

(c) The kernel on the right is F^p.

Moreover, the Kummer pairing induces a perfect bilinear pairing

$$\kappa_+ : G \times B/F^p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Elliptic Curves

We shall now construct the Kummer pairing in the context of elliptic curves. Let E/K be an elliptic curve over K. Let $E(K)$ denote the group of K-rational points on the elliptic curve E. Let $m \geq 2$. In this section we will assume that the m-torsion subgroup $E[m] = \{P \in E \mid [m]P = \mathcal{O}\} \subset E(K)$. By $mE(K) = \{mP \mid P \in E(K)\}$.

Definition The **Kummer pairing** is defined as

$$\kappa_e : E(K) \times \operatorname{Gal}\left(\bar{K}/K\right) \longrightarrow E[m] \text{ where } \kappa(P, \sigma) = \sigma(Q) - Q \text{ where } [m]Q = P.$$

Theorem 11. *Let E/K be an elliptic curve with group $E(K)$ and suppose that $E[m] \subset E(K)$.*

(a) The Kummer pairing κ_e is a well-defined bilinear map;

(b) The kernel of κ_e on the left is $mE(K)$;

(c) The kernel of κ_e on the right is $\mathrm{Gal}\left(\bar{K}/L\right)$ where $L = K\left([m]^{-1}E(K)\right)$ is the compositum of all fields $K(Q)$ as Q ranges over the points $E\left(\bar{K}\right)$ satisfying $[m]Q \in E(K)$.

Hence the Kummer pairing induces a perfect bilinear pairing

$$\kappa_e : E(K)/mE(K) \times \mathrm{Gal}\left(\bar{K}/K\right) \longrightarrow E[m]$$

where L is the field given in (d).

Proof. (a) We first show that $\kappa(P,\sigma) \in E[m]$. Note that

$$[m]\,\kappa(P,\sigma) = [m]\,\sigma(Q) - [m]\,Q = \sigma(P) - P = \mathcal{O}$$

since $P \in E(K)$. If $P = [m]Q$ and $P = [m]R$, then $R = Q + T$ for some $T \in E[m]$ and therefore

$$\sigma(Q+T) - (Q+T) = \sigma(Q) + \sigma(T) - Q - T = \sigma(Q) - Q$$

since $E[m] \subset E(K)$ and so σ fixes T. □

If we consider the isogeny $[m] : E \to E$ where $P \longmapsto [m]P$, then we have that the **Weil pairing** reduces to

$$e_m : E[m] \times E[m] \to \mu_m.$$

We have seen that the Weil pairing is bilinear, non-degenerate, and Galois invariant. With this in mind we show:

Corollary 12. *There exist points $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive m-th root of unity. In particular, if $E[m] \subset E(K)$, then $\mu_m \subset K$.*

Proof. We have that $e_m(E[m] \times E[m]) \subset \mu_m$ is a subgroup. Let's say it is equal to μ_d where $d|n$. Then

$$1 = e_m(S,T)^d = e_m([d]S, T) \text{ for each } S, T \in E[m].$$

Since e_m is non-degenerate, we have that $[d]S = \mathcal{O}$. But then $d = m$ since $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

If $E[m] \subset E(K)$, then the Galois invariance of the Weil-pairing implies that $e_m(S,T) \in K^*$ for each $S, T \in E[m]$. Hence $\mu_m \subset K^*$. □

Since $\mu_m \subset K$, we can consider the Kummer pairing κ. We have that

$$\kappa : \mathrm{Gal}(L/K) \times K^*/K^{*m} \longrightarrow \mu_m$$

is a perfect pairing and so we have an isomorphism

$$\delta_\kappa : K^*/K^{*m} \xrightarrow{\sim} \mathrm{Hom}\left(\mathrm{Gal}\left(\bar{K}/K\right), \mu_m\right) \text{ where } \delta_\kappa(a)(\sigma) = \kappa(\sigma, a).$$

Similarly, we have that the following isomorphism from the Kummer pairing on elliptic curves:

$$\delta_E : E(K)/mE(K) \xrightarrow{\sim} \mathrm{Hom}\left(\mathrm{Gal}\left(\bar{K}/K\right), E[m]\right) \text{ where } \delta_E(P)(\sigma) = \kappa_e(\sigma, P).$$

Theorem 13. *There is a bilinear pairing*

$$b : E(K)/mE(K) \times E[m] \longrightarrow K^*/K^{*m}$$

satisfying

$$e_m(\delta_E(P), T) = \delta_\kappa(b(P,T)).$$

The pairing is nondegenerate on the left.

References

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.