Kummer theory for finite fields

Jean-Marc Couveignes

Institut de Mathématiques de Bordeaux

Workshop FAST, September 2017

The linear sieve

Algorithm for computing discrete logarithms in $\mathbb{F}_q$ with $q = p^d$.
$\mathbb{F}_q = \mathbb{F}_p[X]/A(X)$ with $A(X) \in \mathbb{F}_p[X]$
$A(X)$ unitary, irreducible, degree d.
Set $x = X \bmod A(X)$.
For every $0 \leq n \leq d-1$ set

$$L_n = \mathbb{F}_p \oplus x\mathbb{F}_p \oplus \cdots \oplus x^n\mathbb{F}_p \subset \mathbb{F}_q.$$

So $L_0 = \mathbb{F}_p \subset L_1 \subset \ldots \subset L_{d-1} = \mathbb{F}_q$ and
$L_a \times L_b \subset L_{a+b}$ if $a + b \leq n - 1$.
Fix κ.
Look for multiplicative relations between elements in L_κ.
For example if $\kappa = 1$:

$$\prod_{1 \leq i \leq I} (a_i + b_i x)^{e_i} = 1 \in \mathbb{F}_q \tag{1}$$

with a_i and b_i in $\mathbb{F}_p$.

Finding relations

Once found enough relations we have a basis of the $\mathbb{Z}$-module of relations between elements in L_κ.
How do we find relations like 1 ?
Assume again $\kappa = 1$.
Pick random triples (a_i, b_i, e_i) and compute the residue modulo $A(X)$ of $\prod_i (a_i + b_i X)^{e_i}$:

$$r(X) \equiv \prod_i (a_i + b_i X)^{e_i} \bmod A(X)$$

with $\deg(r(X)) \leq d - 1$.
Hope $r(X)$ splits as $r(X) = \prod_j (u_j + v_j X)^{f_j}$.
We get the relation

$$\prod_i (a_i + b_i x)^{e_i} \prod_j (u_j + v_j x)^{-f_j} = 1.$$

L_κ is called the smoothness base.

A remark by Joux and Lercier

Recall $x = X \bmod A(X)$.
Assume there is an automorphism $\mathfrak{a}$ of $\mathbb{F}_q$ such that $\mathfrak{a}(x) = ux + v$ avec $u, v \in \mathbb{F}_p$,
Letting $\mathfrak{a}$ act on equation 1 we obtain another relation of the same type :

$$\prod_{1 \le i \le I} (a_i + b_i(ux + v))^{e_i} = 1 \in \mathbb{F}_q. \tag{2}$$

Indeed $\mathfrak{a}$ acts not only on equations but also on factors $a_i + b_i x$.
Assuming $\mathfrak{a} = \phi^\alpha$

$$\mathfrak{a}(x) = x^{p^\alpha} = ux + v \in \mathbb{F}_q \tag{3}$$

Remove $ux + v$ out of the smoothness base and replace it in every relation by x^{p^α}.
Divide the size of the smoothness base by the order of the group generated by $\mathfrak{a}$ (at most d).

Degree maps

Strategy : find smoothness bases that are Galois invariant.
In the above case, define the degree of $z = a_0 + a_1 x + \cdots + a_k x^k$ to be k if $0 \leq k < d$ and $a_k \neq 0$.
Smallest k s.t. $z \in L_k$.

- $\deg(z \times t) \leq \deg(z) + \deg(t)$,
- there are p^n elements with degree $< n$ for $n \leq d$,
- there is an algorithm that factors certain elements in $L_{d-1} = \mathbb{F}_q$ as products of elements with smaller degree. There is a significant proportion of such smooth elements.

We look for such degree functions that are Galois invariant.

An example

This example is given by Joux et Lercier :
Take $p = 43$ and $d = 6$ so $q = 43^6$ and let $A(X) = X^6 - 3$ which is irreducible in $\mathbb{F}_{43}[X]$.
So $\mathbb{F}_q = \mathbb{F}_{43}[X]/X^6 - 3$.
Since $p = 43$ is congruent to 1 modulo $d = 6$ we have

$$\phi(x) = x^{43} = (x^6)^7 \times x = 3^7 x = \zeta_6 x$$

with $\zeta_6 = 3^7 = 37 \bmod 43$.
This is Kummer theory. Similar examples are produced by Artin-Schreier theory. What are the limitations of these constructions ?

Kummer theory

Classify cyclic degree d extensions of $\mathbf{K}$ with characteristic p prime to d containing a primitive d-th root of unity.
Embed $\mathbf{K}$ in a Galois closure $\bar{\mathbf{K}}$.
Let H be a subgroup of $\mathbf{K}^*$ containing $(\mathbf{K}^*)^d$.
Set $\mathbf{L} = \mathbf{K}(H^{\frac{1}{d}})$.
One associates to every $\mathfrak{a}$ in $\mathrm{Gal}(\mathbf{K}(H^{\frac{1}{d}})/\mathbf{K})$ an homomorphism $\kappa(\mathfrak{a})$ from $H/(\mathbf{K}^*)^d$ to μ_d

$$\kappa(\mathfrak{a}) : \theta \mapsto \frac{\mathfrak{a}(\theta^{\frac{1}{d}})}{\theta^{\frac{1}{d}}}.$$

The map $\mathfrak{a} \mapsto \kappa(\mathfrak{a})$ is an isomorphism from $\mathrm{Gal}(\mathbf{K}(H^{\frac{1}{d}})/\mathbf{K})$ to $\mathrm{Hom}(H/(\mathbf{K}^*)^d, \mu_d)$.
Classifies abelian extensions of $\mathbf{K}$ with exponent dividing d.

Kummer theory of finite fields

If $\mathbf{K} = \mathbb{F}_q$ then any subgroup H of $\mathbf{K}^*$ is cyclic. We must assume $d|q-1$ and set $q-1 = md$.
We take $H = \mathbf{K}^*$ so $\mathbf{K}^*/(\mathbf{K}^*)^d$ is cyclic with order d corresponding to the unique degree d extension of $\mathbf{K}$:
Let r be a generator of $\mathbf{K}^*$ and

$$s = r^{\frac{1}{d}}.$$

Set $\mathbf{L} = \mathbf{K}(s)$. The Galois group is generated by the Frobenius ϕ and $\phi(s) = s^q$ so

$$\kappa(\phi)(r) = \frac{\phi(s)}{s} = s^{q-1} = \zeta = r^m$$

The map $r \mapsto \zeta$ from $\mathbf{K}^*/(\mathbf{K}^*)^d$ to μ_d is exponentiation by m.

Artin-Schreier theory

Classifies degree p extensions of $\mathbf{K}$.
Here the map $X \mapsto X^d$ is replaced by $X \mapsto X^p - X = \wp(X)$.
One adds to $\mathbf{K}$ the roots of $X^p - X = a$.
Let H be a subgroup of $(\mathbf{K}, +)$ containing $\wp(\mathbf{K})$ and set $\mathbf{L} = \mathbf{K}(\wp^{-1}(H))$.
To every $\mathfrak{a}$ in $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ one associates an homomorphism $\kappa(\mathfrak{a})$ from $H/\wp(\mathbf{K})$ to $(\mathbb{F}_p, +)$:

$$\kappa(\mathfrak{a}) : \theta \mapsto \mathfrak{a}(\wp^{-1}(\theta)) - \wp^{-1}(\theta).$$

The map $\mathfrak{a} \mapsto \kappa(\mathfrak{a})$ is an isomorphism from the Galois group $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ to $\mathrm{Hom}(H/\wp(\mathbf{K}), \mathbb{F}_p)$.

Artin-Schreier for finite fields

Assume $\mathbf{K} = \mathbb{F}_q$ with $q = p^f$.
The kernel of $\wp : \mathbb{F}_q \to \mathbb{F}_q$ is $\mathbb{F}_p$ and the quotient $\mathbb{F}_q/\wp(\mathbb{F}_q)$ has order p.
The unique extension $\mathbf{L}$ of degree p of $\mathbb{F}_q$ is generated by $b = \wp^{-1}(a)$ with $a \in \mathbb{F}_q - \wp(\mathbb{F}_q)$.
$\phi(b) - b$ is in $\mathbb{F}_p$ and the map $a \mapsto \phi(b) - b$ is an isomorphism from $\mathbf{K}/\wp(\mathbf{K})$ to $\mathbb{F}_p$.
More explicitly $\phi(b) = b^q$ and
$\phi(b) - b = b^q - b = (b^p)^{p^{f-1}} - b = (b+a)^{p^{f-1}} - b$ since
$\wp(b) = b^p - b = a$.
So $b^{p^f} - b = b^{p^{f-1}} - b + a^{p^{f-1}}$ and iterating we obtain

$$\phi(b) - b = b^{p^f} - b = a + a^p + a^{p^2} + \cdots + a^{p^{f-1}}.$$

So the isomorphism from $\mathbf{K}/\wp(\mathbf{K})$ to $\mathbb{F}_p$ is the absolute trace.

Invariant flags of linear spaces

Kummer : $\mathbf{L} = \mathbf{K}[x]$ with $x^d = r$
$L_k = \mathbf{K} \oplus \mathbf{K}x \oplus \cdots \oplus \mathbf{K}x^k$ is Galois invariant since $\mathfrak{a}(x) = \zeta x$ and $\zeta \in \mathbf{K}$.
We have a Galois invariant flag
$\mathbf{K} = L_0 \subset L_1 \subset \cdots \subset L_{d-1} = \mathbf{L}$
of vector spaces.
Artin-Schreier : $\mathbf{L} = \mathbf{K}[x]$ with $x^p - x = a$ and $\mathfrak{a}(x) = x + c$ with $c \in \mathbf{K}$ so $\mathfrak{a}(x^k) = (x + c)^k \in L_k$.
This time the Galois action is triangular rather than diagonal. Same phenomenon for Witt-Artin-Schreier extensions.
In both cases we have a Galois invariant degree function.

Invariant flags of linear spaces

Which cyclic extensions $\mathbf{L}/\mathbf{K}$ allow such a Galois invariant flag of vector spaces ?
Let C be the (cyclic) Galois group and d its order.
Assume d is prime to p. Let ϕ be a generator of C.
Let $(w, \phi(w), \phi^2(w), \dots, \phi^{d-1}(w))$ be a normal $\mathbf{K}$-base of $\mathbf{L}$.
For every irreducible factor $f \in \mathbf{K}[X]$ of $X^d - 1$, call $V_f \subset \mathbf{L}$ the associated characteristic subspace in $\mathbf{L}$.
Every Galois invariant $\mathbf{K}$-linear space in $\mathbf{L}$ is a direct sum of such characteristic spaces.
If a complete Galois invariant flag exists

$$\mathbf{K} = L_0 \subset L_1 \subset \cdots \subset L_{d-1} = \mathbf{L}$$

with L_k of dimension k, then every f must have degree 1. So $X^d - 1$ splits on $\mathbf{K}$ and we are in the Kummer case.

Specializing isogenies between algebraic groups

Le $\mathbf{G}/\mathbf{K}$ be a commutative algebraic group over a perfect field and $T \subset \mathbf{G}(\mathbf{K})$ a finite subgroup and

$$I : \mathbf{G} \to \mathbf{H}$$

the quotient by T.
Set $d = \#T = \deg(I)$.
Assume there is a $\mathbf{K}$-rational point a in $\mathbf{H}$ such that $I^{-1}(a)$ is irreducible.
Any $b \in \mathbf{G}(\bar{\mathbb{F}}_p)$ such that $I(b) = a$ defines a degree d cyclic extension $\mathbf{L} = \mathbf{K}(b)$ of $\mathbf{K}$. Indeed we have a non-degenerate pairing

$$<,>: H(\mathbf{K})/I(G(\mathbf{K})) \times \mathrm{Gal}(I^{-1}(H(\mathbf{K}))) \to T$$

If $a \in H(\mathbf{K})$ take $b \in I^{-1}(a)$ and set $< a, \mathfrak{a} >= \mathfrak{a}(b) - b$.

Geometric automorphisms

Automorphisms of $\mathbf{K}(b)/\mathbf{K}$ admit a geometric description. They act by translation.
Let ϕ be a generator of $\mathrm{Gal}(\mathbf{K}(b)/\mathbf{K})$. There is a $t \in T$ such that

$$\phi(b) = b \oplus_{\mathbf{G}} t.$$

Kummer : $\mathbf{G} = \mathbf{H} = \mathbf{G}_{\mathrm{m}}$ and $I = [d]$.
See $\mathbf{G} \subset \mathbb{A}^1$ with z-coordinate and $z(0_{\mathbf{G}}) = 1$ and
$z(P_1 \oplus_{\mathbf{G}_{\mathrm{m}}} P_2) = z(P_1) \times z(P_2)$, $z(I(P)) = z(P)^d$, $z(t) = \zeta$,
$z(b \oplus_{\mathbf{G}_{\mathrm{m}}} t) = \zeta \times z(b)$.

Artin-Schreier : $\mathbf{G} = \mathbf{H} = \mathbf{G}_{\mathrm{a}}$ and $I = \wp$
See $\mathbf{G}_{\mathrm{a}} = \mathbb{A}^1$ with z-coordinate $z(0_{\mathbf{G}}) = 0$ and
$z(P_1 \oplus_{\mathbf{G}_{\mathrm{a}}} P_2) = z(P_1) + z(P_2)$, $z(\wp(P)) = z(P)^p - z(P)$,
$z(P \oplus_{\mathbf{G}_{\mathrm{a}}} t) = z(P) + c$ where $c = z(t) \in \mathbb{F}_p$.

A different example

We first take $\mathbf{G}$ to be the Lucas torus. Assume p is odd.
Let D be a non-zero element in $\mathbf{K}$.
Let $\mathbb{P}^1$ be the projective line with homogeneous coordinates $[U, V]$ and affine coordinate $u = \frac{U}{V}$.
$\mathbf{G} \subset \mathbb{P}^1$ is the open subset with inequation

$$U^2 - DV^2 \neq 0.$$

$u(0_{\mathbf{G}}) = \infty$ and $u(P_1 \oplus_{\mathbf{G}} P_2) = \frac{u(P_1)u(P_2)+D}{u(P_1)+u(P_2)}$ and
$u(\ominus_{\mathbf{G}} P_1) = -u(P_1)$.
Assume $\mathbf{K} = \mathbb{F}_q$ and D is not a square in $\mathbb{F}_q$.
$\#\mathbf{G}(\mathbb{F}_q) = q + 1$ and $u \in \mathbb{F}_q \cup \{\infty\}$.
The Frobenius endomorphism $\phi : [U, V] \mapsto [U^q, V^q]$ is nothing but multiplication by $-q$.
Indeed

$$(U + V\sqrt{D})^q = U^q - \sqrt{D}V^q$$

because D is not a square $\mathbb{F}_q$.

Using the Lucas Torus

If d divides $q+1$ then $\mathbf{G}[d]$ is $\mathbb{F}_q$-rational.
Set $q+1 = md$ and consider the isogeny $I = [d] : \mathbf{G} \to \mathbf{G}$.
The quotient $\mathbf{G}(\mathbb{F}_q)/I(\mathbf{G}(\mathbb{F}_q)) = \mathbf{G}(\mathbb{F}_q)/\mathbf{G}(\mathbb{F}_q)^d$ is cyclic of order d. Let r be a generator of $\mathbf{G}(\mathbb{F}_q)$ and choose $s \in I^{-1}(r)$.
Let $\mathbf{L} = \mathbf{K}(s) = \mathbf{K}(u(s))$ a degree d extension of $\mathbf{K}$.
For any $\mathfrak{a} \in \mathrm{Gal}(\mathbf{L}/\mathbf{K})$, the difference $\mathfrak{a}(s) \ominus_{\mathbf{G}} s$ lies in $\mathbf{G}[d]$ and the pairing

$$< \mathfrak{a}, r > \mapsto \mathfrak{a}(s) \ominus_{\mathbf{G}} s$$

induces an isomorphism from $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ to $\mathrm{Hom}(\mathbf{G}(\mathbf{K})/(\mathbf{G}(\mathbf{K}))^d, \mathbf{G}[d])$.
Here $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ is generated by ϕ and $< \phi, r >$ is $\phi(s) \ominus_{\mathbf{G}} s$.
Remember that $\phi(s) = [-q]$ so

$$(\phi, r) = [-q-1]s = [-m]r.$$

Lucas polynomials

Call σ the u-coordinate of s and τ the one of t then

$$\phi(\sigma) = \frac{\tau\sigma + D}{\sigma + \tau}$$

and the Frobenius acts like a linear rational transform.
Let $A(X) = \prod_{s \in I^{-1}(r)}(X - u(s))$ be the minimal polynomial of $u(s)$ and set $\mathbf{L} = \mathbf{K}[X]/A(X)$.
One has $(U + \sqrt{D}V)^d = \sum_{0 \leq 2k \leq d} \left(\begin{array}{c} d \\ 2k \end{array} \right) U^{d-2k} V^{2k} D^k + \sqrt{D} \sum_{1 \leq 2k+1 \leq d} \left(\begin{array}{c} d \\ 2k+1 \end{array} \right) U^{d-2k-1} V^{2k+1} D^k$.

So $u([k]P) = \dfrac{\sum_{0 \leq 2k \leq d} u(P)^{d-2k} \left(\begin{array}{c} d \\ 2k \end{array} \right) D^k}{\sum_{1 \leq 2k+1 \leq d} u(P)^{d-2k-1} \left(\begin{array}{c} d \\ 2k+1 \end{array} \right) D^k}$

A non-linear flag

$$A(X) = \sum_{0\leq 2k\leq d} X^{d-2k} \left(\begin{array}{c} d \\ 2k \end{array} \right) D^k - u(r) \sum_{1\leq 2k+1\leq d} X^{d-2k-1} \left(\begin{array}{c} d \\ 2k+1 \end{array} \right) D^k.$$

Set $x = X \bmod A(X)$. The Galois group acts on x by linear rational transforms so it is sensible to define for every $k < d$

$$P_k = \{ \frac{a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k}{b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k} | (a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_k) \in \mathbf{K}^{2k+2} \}.$$

One has

$$\mathbf{K} = P_0 \subset P_1 \subset \cdots \subset P_{d-1} = \mathbf{L}$$

and the the P_k are Galois invariant.
Further

$$P_k \times P_l \subset P_{k+l}$$

if $k + l \leq d - 1$.

An example

Take $p = q = 13$ and $d = 7$ so $m = 2$. Check $D = 2$ is not a square in $\mathbb{F}_{13}$.
Find $r = U + \sqrt{2}V$ such that r has order $p + 1 = 14$ in $\mathbb{F}_{13}(\sqrt{2})^*/\mathbb{F}_{13}^*$.
For example $U = 3$ et $V = 2$ are fine.
The u-coordinate of $3 + 2\sqrt{2}$ is $u(r) = \frac{3}{2} = 8$.

$$A(X) = X^7 + 3X^5 + 10X^3 + 4X - 8(7X^6 + 5X^4 + 6X^2 + 8).$$

Set $t = [-m]r = [-2]r$ so $u(t) = 4$. Since Frobenius acts like translation by t :

$$X^p = \frac{4X + 2}{X + 4} \bmod A(X).$$

Références

N. Bourbaki.
Algèbre, chapitre V.
Masson, 1981.

A. Joux and R. Lercier.
The function field sieve in the medium prime case.
Lecture Notes in Comput. Sci., 4004 :254–270, 2006.

S. Lang.
Algebra.
Addison-Wesley, 1984.

G. Malle and B.H. Matzat.
Inverse Galois Theory.
Springer, 1999.

A. M. Odlyzko.
Discrete logarithms : The past and the future.
Designs, Codes, and Cryptography, 19 :129–145, 2000.

Using elliptic curves

This time we take $\mathbf{G} = E/\mathbb{F}_q$ an ordinary elliptic curve.
Let $\mathfrak{i}$ be a degree d ideal of $\mathrm{End}(E)$ dividing $\phi - 1$.
Assume $\mathfrak{i}$ is invertible and $\mathrm{End}(E)/\mathfrak{i}$ is cyclic.
Set $T = \mathrm{Ker}\,\mathfrak{i} \subset E(\mathbb{F}_q)$ and $I : E \to F = E/T$.
The quotient $F(\mathbb{F}_q)/I(E(\mathbb{F}_q))$ is isomorphic to T.
Choose a in $F(\mathbb{F}_q)$ such that $a \bmod I(E(\mathbb{F}_q))$ is a generator.
Choose $b \in I^{-1}(a)$ and set $\mathbf{L} = \mathbf{K}(b)$ a degree d extension.
Clearly $\phi(b) = b \oplus_{\mathbf{G}} t$ for some $t \in T$.
For any integer $k \geq 0$ call $\mathcal{F}_k$ the set of functions in $\mathbb{F}_q(E)$ with degree $\leq k$ having no pole at b.

$$P_k = \{f(b) | f \in \mathcal{F}_k\}.$$

Clearly $\mathbf{K} = P_0 = P_1 \subset P_2 \subset \cdots \subset P_d = \mathbf{L}$ and

$$P_k \times P_l \subset P_{k+l}.$$

Since $\mathcal{F}_k$ is invariant by T, also P_k is invariant by $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ because $\phi(f(b)) = f(\phi(b)) = f(b \oplus_{\mathbf{G}} t)$.