Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

33- Monday November 21, 2011.

Lemma 33.1: Splitting fields are unique up to isomorphism. More precisely, if σ is an isomorphism from E_1 onto E_2, if F_1 is a splitting field extension for $P_1 \in E_1[x]$ over E_1, and F_2 is a splitting field extension for $P_2 = \sigma\, P_1 \in E_2[x]$ over E_2, then there exists an isomorphism τ from F_1 onto F_2 extending σ.[1] It follows that $[F_1\!:\!E_1] = [F_2\!:\!E_2]$. If $E_2 = E_1$ and $\sigma = id_{E_1}$, then the isomorphism τ fixes E_1. If $F_2 = F_1$, τ is an automorphism of F_1 which moves E_1 to E_2.
Proof: By induction on the dimension $[F_1\!:\!E_1]$.[2] If $[F_1\!:\!E_1] = 1$, then $F_1 = E_1$ and P_1 splits over E_1, i.e. $P_1 = c\,\prod_{i=1}^d (x-a_i)$ with $c \in E_1^*$, $a_1,\ldots,a_d \in E_1$, so that $P_2 = \sigma\,P_1 = \sigma(c)\,\prod_{i=1}^d \big(x-\sigma(a_i)\big)$ with $\sigma(c) \in E_2^*$, $\sigma(a_1),\ldots,\sigma(a_d) \in E_2$, i.e. P_2 splits over E_2, hence $F_2 = E_2$.

If $[F_1\!:\!E_1] > 1$, let $a \in F_1 \setminus E_1$ be a root of P_1 (which exists, since F_1 is generated by these roots), so that a is algebraic over E_1 (since $P_1(a) = 0$), and let $P \in E_1[x]$ be the monic irreducible polynomial with $P(a) = 0$, so that P divides P_1; one then defines $Q = \sigma\,P$. Since P divides P_1, one deduces that Q divides P_2, so that Q splits over F_2, and there exists $a' \in F_2$ (among the roots of P_2) such that $Q(a') = 0$, hence the monic irreducible polynomial in $E_2[x]$ associated to a' divides Q; then, there exists an isomorphism ρ from $E_1(a)$ onto $E_2(a')$ extending σ and such that $\rho(a) = a'$ by Lemma 32.2. Then, if $P_1 = (x-a)\,Q_1$ and $P_2 = (x-a')\,Q_2$, one has $Q_2 = \sigma\,Q_1$, and one checks easily that F_1 is a splitting field extension for Q_1 over $E_1(a)$,[3] and that F_2 is a splitting field extension for P_2 over $E_2(a')$, and one applies the induction hypothesis for constructing an isomorphism τ, since $[F_1\!:\!E_1] = [F_1\!:\!E_1(a)]\,[E_1(a)\!:\!E_1]$ and $[E_1(a)\!:\!E_1] > 1$ gives $[F_1\!:\!E_1(a)] < [F_1\!:\!E_1]$.

Lemma 33.2: For any prime p and any $k \ge 1$, two fields of size $q = p^k$ are isomorphic.
Proof: If F is a finite field of characteristic p, and F_0 is its prime subfield, isomorphic to $\mathbb{Z}_p$, then $|F| = q = p^k$ means $[F\!:\!F_0] = k$. Since F^* is a finite multiplicative group of order $q-1$, one has $a^{q-1} = 1$ for all $a \in F^*$, so that $a^q = a$ for all $a \in F$. Since $x^q - x$ is a monic polynomial of degree q and one knows q distinct roots, one has $x^q - x = \prod_{a\in F}(x-a)$, and F is then a splitting field extension for $x^q - x$ over F_0, since the polynomial splits over F and its roots certainly generate F, because every element of F is a root. Since splitting field extensions are unique up to isomorphism by Lemma 33.1, two such fields are isomorphic.

Lemma 33.3: Let D be any field of characteristic p, with D_0 as prime subfield ($\simeq \mathbb{Z}_p$). Then, the mapping φ_p, defined by $\varphi_p(a) = a^p$ for all $a \in D$, is an *injective* ring-homomorphism from D into itself. If D is finite, it is an automorphism, the *Frobenius automorphism*,[4] with *fixed field* D_0.[5]
Proof: Since $\varphi_p(a+b) = (a+b)^p = a^p + \big(\sum_{j=1}^{p-1} \binom{p}{j}\, a^j\, b^{p-j}\big) + b^p$ and the binomial coefficient $\binom{p}{i}$ is a multiple of p except for $i = 0$ and $i = p$ because p is prime, the right side is $a^p + b^p$, i.e. $\varphi_p(a) + \varphi_p(b)$; then $\varphi_p(a\,b) = (a\,b)^p = a^p b^p = \varphi_p(a)\,\varphi_p(b)$, so that φ_p is a ring-homomorphism.

If $\varphi_p(a) = \varphi_p(b)$, then $\varphi_p(b-a) = \varphi_p(b) + \varphi_p(-1)\,\varphi_p(a) = \varphi_p(b) - \varphi_p(a) = 0$ (since $p = 2$ implies $+1 = -1$), and $(b-a)^p = 0$ implies $b = a$. If D is finite, any injective mapping from D into itself is also surjective. By Fermat's theorem, $j^{p-1} = 1 \pmod p$ for $j = 1,\ldots,p-1$, so that $a^{p-1} = 1$ for all $a \in D_0^*$, hence $a^p = a$ for all $a \in D_0$, i.e. $\varphi_p(a) = a$; since $x^p - x$ has degree p and one already knows p distinct roots, one knows them all, and $\varphi_p(x) = x$ implies $x \in D_0$.

---

[1] This isomorphism τ is not unique in general, as seen from the proof, where one chooses a root of Q.

[2] One has $[F_1\!:\!E_1] < \infty$: if $a_1,\ldots,a_d$ are the roots of P_1 in F_1, then each a_j is algebraic over E_1 with an order $\le d$, so that $[F_1\!:\!E_1]$ is at most the product of the orders, giving an upper bound d^d. Once the result is proved, it is at most $d!$ since a splitting field extension was constructed satisfying such a bound.

[3] Because Q_1 splits over F_1, and the smallest field containing $E_1(a)$ and all the roots of Q_1 contains E_1 and all the roots of P_1, and is then F_1.

[4] Ferdinand Georg FROBENIUS, German mathematician, 1949–1918. He worked in Berlin, Germany.

[5] The fixed points of an endomorphism ψ of a ring R is a subring of R, since $\psi(x) = x$ and $\psi(y) = y$ imply $\psi(x+y) = \psi(x) + \psi(y) = x + y$, so that $\psi(0) = 0$ and $\psi(-x) = -\psi(x)$, and $\psi(x\,y) = \psi(x)\,\psi(y) = x\,y$. The fixed points of an automorphism ψ of a field K is a subfield of K, since $\psi(x) = \psi(x)\,\psi(1)$ for all $x \in K$ implies $\psi(1) = 1$, and $x^{-1}\,x = 1$ for $x \neq 0$ implies $\big(\psi(x)\big)^{-1}\psi(x) = 1$, so that $\psi(x) = x \neq 0$ implies $\psi(x^{-1}) = x^{-1}$.

Lemma 33.4: Let $E = \mathbb{Z}_p$, and for $k \geq 1$ let F be a splitting field extension for $Q = x^{p^k} - x$ over E. Then $|F| = p^k$.
Proof: Since $Q' = -1$, there are no multiple roots in F, and since $[F:E] < \infty$, F is finite and the Frobenius mapping φ_p is an automorphism by Lemma 33.3, fixing E by Fermat's theorem, i.e. $\varphi_p \in Aut_E(F)$, hence $\varphi_p^k \in Aut_E(F)$, and $\varphi_p^k(x) = x^{p^k}$ for all x (because product means composition), the fixed field of φ_p^k is then exactly the roots of Q, which is then the smallest field containing E and the roots of Q, i.e. F, and this shows that $|F| = p^k$.

Remark 33.5: It is common to call F_q a field of order q, with q a power of a prime p, so that F_p is then isomorphic to $\mathbb{Z}_p$.

This is a third different meaning for the notation F_n, but it denotes now a finite field (only used if $n = p^k$ for a prime p), while the first two denoted integers, the nth Fibonacci number (with $F_0 = F_1 = 1$ and $F_{n+2} = F_n + F_{n+1}$ for all $n \geq 0$), or the nth Fermat "prime" ($F_n = 2^{2^n} + 1$, which is only known to be prime for $0 \leq n \leq 4$).

Lemma 33.6: If E is any field, and G is a *finite* subgroup of the multiplicative group $E^* = E \setminus \{0\}$, then G is cyclic.
Proof: Because G is finite, every element has a finite order; let ℓ be the *lcm* (least common multiple) of the orders of the elements of G, so that $g^\ell = 1$ for all $g \in G$. By the structure theorem for finite Abelian groups, there is an element g_0 of order ℓ,[6] so that G has at least ℓ elements, but on the other hand $x^\ell = 1$ has at most ℓ roots, so that G has exactly ℓ elements and is generated by g_0.

Definition 33.7: If E is a field and F is a finite field extension of E, with $[F:E] = k$, a *power basis* is a basis of F (as an E-vector space) which has the form $\{1, a, \ldots, a^{k-1}\}$ for an element $a \in F$.

Remark 33.8: Using Lemma 33.6, we shall prove that a power basis exists for any finite field F_q (if E is its prime subfield, isomorphic to $\mathbb{Z}_p$ if $q = p^k$).

From a practical point of view, finite fields are important in coding theory and in cryptography, and a power basis is often used, but implicitly as a root of an irreducible polynomial, so that one encounters the question of irreducible polynomial in $\mathbb{Z}_p[x]$, for example. In case of $\mathbb{Z}_2$, I found written that the irreducible polynomials are $x^2 + x + 1$ if $k = 2$, $x^3 + x + 1$ or $x^3 + x^2 + 1$ if $k = 3$, $x^4 + x + 1$ or $x^4 + x^3 + 1$ if $k = 4$, and that some irreducible polynomials for $k \geq 5$ are $x^5 + x^2 + 1$ if $k = 5$, $x^6 + x + 1$ if $k = 6$, $x^7 + x + 1$ if $k = 7$, $x^8 + x^4 + x^3 + x^2 + 1$ if $k = 8$, so that there are various practical aspects to consider, like how to check that any of these given polynomials is indeed irreducible, or how to find an irreducible polynomial in a situation which is not listed in the books.

The values used in coding theory are reasonable low for p and for k, and the study of *cyclotomic polynomials* will be of great help, but the values of p used in cryptography have a few hundred digits, and the questions for such cases are then quite different.

[6] Directly, using additive notation, if in an Abelian group H an element a of order n, and if m divides n, then $b = \frac{n}{m}\,a$ has order m. If $(q, r) = 1$ and an element g has order q and another element h has order r, then the cyclic group generated by g and the cyclic group generated by h only intersect at 0, and $g + h$ has order $q\,r$.