21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

31- Wednesday November 16, 2011.

Remark 31.1: If $E_1 = \mathbb{Q}$, $E_2 = \mathbb{Q}[\sqrt[3]{2}]$ and $E_3 = E_2[\sqrt{-3}]$, then E_3 contains $\omega = \frac{-1+\sqrt{-3}}{2}$ and $\omega^2 = \frac{-1-\sqrt{-3}}{2}$, so that it contains the three roots of x^3-2; E_3 is generated by E_1 and the three roots, because E_1 and $\sqrt[3]{2}$ generate E_2, and since any field containing the three roots must contain the ratio of two distinct roots, which is either ω or ω^2, so that the field contains $\sqrt{-3}$, and then E_2 and $\sqrt{-3}$ generate E_3, and it means that E_3 is a splitting field extension for x^3-2 over $\mathbb{Q}$.

Since an element of the Galois group $Aut_{E_1}(E_3)$ must permute the three roots of x^3-2, the Galois group is a subgroup of the symmetric group S_3 of permutations of these three roots, and for showing that it is isomorphic to S_3, one exhibits a transposition τ and a cyclic permutation σ (and then the group generated by τ and ω is S_3).

$E_3 = \mathbb{Q}[\sqrt[3]{2},\sqrt{-3}]$ may be considered as $\{z = a + b\sqrt[3]{2} + c\sqrt[3]{4} + (d + e\sqrt[3]{2} + f\sqrt[3]{4})\sqrt{3}\,i \mid a,b,c,d,e,f \in \mathbb{Q}\} \subset \mathbb{C}$, in which case τ is complex conjugation, defined by $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ and $\tau(\sqrt{-3}) = -\sqrt{-3}$, i.e. , and $\tau(z) = a + b\sqrt[3]{2} + c\sqrt[3]{4} - (d + e\sqrt[3]{2} + f\sqrt[3]{4})\sqrt{3}\,i$, so that $\tau \neq id$ and $\tau\circ\tau = id$.

For defining a cyclic permutation σ, one defines it so that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$, $\sigma(\sqrt[3]{2}\,\omega) = \sqrt[3]{2}\,\omega^2$, and $\sigma(\sqrt[3]{2}\,\omega^2) = \sqrt[3]{2}$, which means $\sigma(\omega) = \omega$ (and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$): one writes $E_3 = \mathbb{Q}[\sqrt[3]{2},\omega] = \{z = a + b\sqrt[3]{2} + c\sqrt[3]{4} + (d + e\sqrt[3]{2} + f\sqrt[3]{4})\,\omega \mid a,b,c,d,e,f \in \mathbb{Q}\}$, and then $\sigma(z) = a + b\sqrt[3]{2}\,\omega + c\sqrt[3]{4}\,\omega^2 + (d + e\sqrt[3]{2}\,\omega + f\sqrt[3]{4}\omega^2)\,\omega$, gives $\sigma \neq id$ and $\sigma\circ\sigma\circ\sigma = id$.

Lemma 31.2: $Aut_{\mathbb{Q}}(\mathbb{R}) = \{id\}$, and $Aut_{\mathbb{R}}(\mathbb{C}) = \{id,\bar{\cdot}\} \simeq S_2$.
Proof: Let $\sigma \in Aut_{\mathbb{Q}}(\mathbb{R})$, i.e. $\sigma(a+b) = \sigma(a) + \sigma(b)$ and $\sigma(a\,b) = \sigma(a)\,\sigma(b)$ for all $a,b \in \mathbb{R}$, and $\sigma(q) = q$ for all $q \in \mathbb{Q}$, and σ is a bijection of $\mathbb{R}$ onto itself. Then, if $x \in \mathbb{R}$ with $x \geq 0$, one has $x = y^2$ for $y = \sqrt{x}$, and $\sigma(x) = \big(\sigma(y)\big)^2 \geq 0$, which implies that σ is non-decreasing (and it must be increasing since it is a bijection), and since $\sigma(q) = q$ for all $q \in \mathbb{Q}$ one deduces that $\sigma(r) = r$ for all $r \in \mathbb{R}$.[1]

Since $\big(\sigma(i)\big)^2 = \sigma(i^2) = \sigma(-1) = -1$, one deduces that $\sigma(i) = \pm i$. Then, for $a,b \in \mathbb{R}$ one has $\sigma(a+b\,i) = \sigma(a) + \sigma(b)\,\sigma(i) = a + b\,\sigma(i)$, so that σ is identity if $\sigma(i) = +i$, and σ is complex conjugation if $\sigma(i) = -i$.

Lemma 31.3: Let $P \in E[x]$ have degree n. Then, there exists a splitting field extension F for P over E satisfying $[F\!:\!E] \leq n!$ (it will be shown that two splitting field extensions for P over E are isomorphic).
Proof: By induction on n. If $n = 1$, take $F = E$. If $n > 1$, let $Q \in E[x]$ be irreducible and divide P, and let $E_1 = E(\alpha)$ with $Q(\alpha) = 0$, i.e. $E_1 = E[x]/(Q)$ and $\alpha = x$, so that $[E_1\!:\!E] = deg(Q) \leq n$. Then, $P \in E_1[x]$ and $P(\alpha) = 0$, so that $P = (x-\alpha)\,R$ with $R \in E_1[x]$, and by the induction hypothesis, there exists a splitting field extension F for R over E_1 satisfying $[F\!:\!E_1] \leq (n-1)!$. One checks easily that F is a splitting field extension for P over E,[2] and it satisfies $[F\!:\!E] = [F\!:\!E_1]\,[E_1\!:\!E] \leq n!$.

Remark 31.4: The proof of Lemma 31.3 shows that if $P = c\,P_1^{m_1}\cdots P_k^{m_k}$ where $c \in E^*$, $m_1,\ldots,m_k \geq 1$, and $P_1,\ldots,P_k \in E[x]$ are distinct monic irreducible polynomials, then one constructs a splitting field extension F for P over E by constructing a splitting field extension for $Q = P_1\cdots P_k$. Then, instead of the bound $\big(deg(Q)\big)! = \big(deg(P_1) + \ldots + deg(P_k)\big)!$ for $[F\!:\!E]$ given by Lemma 31.3, one obtains a better bound $[F:E] \leq deg(P_1)!\cdots deg(P_k)!$ by successively constructing a splitting field extension F_1 for P_1 over E, a

[1] Notice that there is no hypothesis of continuity on σ, since the notion of automorphism is purely algebraic. Actually, the order structure of $\mathbb{R}$ implies that there are only two ring-homomorphisms from $\mathbb{R}$ into itself, 0 and id: indeed, if σ is a ring-homomorphism, then it is non-decreasing since $x \geq 0$ implies $x = y^2$ so that $\sigma(x) = \big(\sigma(y)\big)^2 \geq 0$; then, $\sigma(1) = \sigma(1^2) = \big(\sigma(1)\big)^2$ implies that $\sigma(1)$ is 0 or 1; finally, for $n \in \mathbb{Z}$ one then has $\sigma(n) = n\,\sigma(1)$, and for $q = \frac{a}{b} \in \mathbb{Q}$ one has $b\,\sigma(q) = \sigma(b\,q) = \sigma(a) = a\,\sigma(1)$, so that $\sigma(q) = q\,\sigma(1)$ for all $q \in \mathbb{Q}$; then, since σ is non-decreasing on $\mathbb{R}$, one deduces that $\sigma(r) = r\,\sigma(1)$ for all $r \in \mathbb{R}$.

[2] Since P splits over F, and the field generated by E and the roots of P must contain α, so that it contains $E_1 = E(\alpha)$, then it must contain E_1 and the roots of R, i.e. it must contain F, since F is a splitting field extension for R over E_1.

splitting field extension F_2 for P_2 over F_1, and so on. In particular, for $E = \mathbb{R}$ (where irreducible polynomials have degree 1 or 2), if $deg(P) = 2m$ or $2m+1$, then $[F\!:\!E] \leq 2^m$ (instead of $(2m)!$ or $(2m+1)!$).

Remark 31.5: A first step before proving that two splitting field extensions for $P \in E[x]$ over E are isomorphic, is to observe that when one adds to a field E a root of an irreducible polynomial $P \in E[x]$, it does not matter which root one adds. It might be counter-intuitive in the case of $P = x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible, since one tends to think in terms of complex numbers and make a difference between the root $a = \sqrt[3]{2}$ which is real so that $F_1 = \mathbb{Q}[\sqrt[3]{2}] = \{z = a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$, and the other two roots, $a\,\omega$ and $a\,\omega^2$ with $\omega = \frac{-1+\sqrt{3}\,i}{2}$, which are not real, so that $F_2 = \mathbb{Q}[\sqrt[3]{2}\,\omega] = \{z = a + b\sqrt[3]{2}\,\omega \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ and $\not\subset \mathbb{R}$; however, F_1 and F_2 are isomorphic, and defining ψ by $\psi(a + b\sqrt[3]{2}) = a + b\sqrt[3]{2}\,\omega$ for all $a, b \in \mathbb{Q}$ obviously gives an isomorphism ψ from F_1 onto F_2. Lemma 32.2 will imply the natural generalization, that two splitting field extensions for a polynomial $P \in E[x]$ over E are isomorphic, and it will be useful for proving that (up to isomorphism) there is only one field of size $q = p^k$ for each prime p and each integer $k \geq 1$.

Remark 31.6: In his work on constructing a regular polygon with n sides with straightedge and compass, GAUSS had already seen the importance of having a tower of field extensions of $\mathbb{Q}$ on one side, and a corresponding family of subgroups on the other side, but GALOIS went much further since he considered a more general question, because in the question of solvability one is led to introduce the splitting field extensions (over various fields) for polynomials $x^k - a$ for any $k \geq 2$, and not just for quadratic polynomials $x^2 - a$.

GALOIS must have realized that if a formula for giving the root of a polynomial exists, then it must apply to all the roots, since one should not be able to distinguish between the roots which one has to add. Certainly, one should add all the roots, hence the notion of a splitting field extension, which appears a crucial notion for the correspondence between an *intermediate field* K (i.e. such that $E \subset K \subset F$) and a subgroup of the Galois group $Aut_E(F)$: given K, the corresponding Galois group $Aut_K(F)$ is a subgroup of $Aut_E(F)$, but is every subgroup obtained?

In the question of adding a root of an irreducible polynomial, GAUSS had already considered the case of the polynomial $1 + x + \ldots + x^{p-1}$ for a prime p (a particular case of a *cyclotomic polynomial*), but his proof of irreducibility did not have the elegance of using “Eisenstein's criterion” after the change $x = 1 + y$;[3] actually, this criterion had actually been introduced before EISENSTEIN by SCHÖNEMANN.[4]

[3] Since $1 + x + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \sum_{k=1}^{p} \binom{p}{k} y^{k-1}$, for which “Eisenstein's criterion” applies.

[4] Theodor SCHÖNEMANN, German mathematician, (1812–1868). He proved “Hensel's lemma” before HENSEL, and “Eisenstein's criterion” before EISENSTEIN.