21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

31- Monday April 9, 2012.

Remark 31.1: We have seen some basic properties of field extensions.

A field extension F of a field E is an E-vector space, with dimension denoted $[F:E]$, and if G is a field extension of F one has $[G:E] = [G:F]\,[F:E]$. This permitted to show that the duplication of a cube (i.e. computing $\sqrt[3]{2}$) or the trisection of a $60°$ angle (i.e. computing $\cos 20°$) is not possible by straightedge and compass.

For every polynomial $P \in E[x]$ there exists a splitting field extension F for P over E, i.e. an extension where P splits (i.e. is a product of polynomials of degree 1 in $F[x]$) and F is generated by E and the roots of P; moreover, two splitting field extensions are isomorphic.

In order to deduce that up to isomorphism there is a unique finite field F_q of order $q = p^k$ for a prime p and $k \geq 1$, it was noticed that every finite subgroup of the multiplicative group K^* of a field K is cyclic, so that F_q must be a splitting field extension over $F_p \simeq \mathbb{Z}_p$ of $P = x^{q-1} - 1$. Moreover, using a generator of the multiplicative group $F_{q^r}^*$, it was noticed that the exists a power basis for F_{q^r} over F_q.

I had not developed more about Galois theory (which will be discussed now) since my purpose was to derive the properties of finite fields in order to use them in questions of coding, and ascertain how much of Galois theory is really needed for such applications.

Definition 31.2: For a field extension F of E, recall that the Galois group $Aut_E(F)$ is the group (for composition) of automorphisms of F which fix all the elements of E. F is called a *Galois extension of* E if $[F:E] < \infty$ and $\{f \in F \mid \sigma(f) = f \text{ for all } \sigma \in Aut_E(F)\} = E$.

Remark 31.3: One checks easily that $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ are Galois extensions of $\mathbb{Q}$, and that $\mathbb{C}$ is a Galois extension of $\mathbb{R}$, but that neither $\mathbb{Q}[\sqrt[3]{2}]$ nor $\mathbb{R}$ are Galois extensions of $\mathbb{Q}$.

For $F = \mathbb{Q}[\sqrt{2}]$, $Aut_{\mathbb{Q}}(F) = \{id, \sigma\}$ with $\sigma(\sqrt{2}) = -\sqrt{2}$. For $F = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $Aut_{\mathbb{Q}}(F) = \{id, \sigma, \tau, \sigma\,\tau\}$ with $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}$, and $\tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$. For $F = \mathbb{C}$, $Aut_{\mathbb{R}}(F) = \{id, \sigma\}$ with $\sigma(i) = -i$.

For $F = \mathbb{Q}[\sqrt[3]{2}]$, and $\sigma \in Aut_{\mathbb{Q}}(F)$, $\sigma(\sqrt[3]{2})$ must be a root of $x^3 = 2$, but since $F \subset \mathbb{R}$, the only root is $\sqrt[3]{2}$, so that $\sigma = id$. For $F = \mathbb{R}$, then $[F:\mathbb{Q}] = \aleph_0$, but also the only $\sigma \in Aut_{\mathbb{Q}}(\mathbb{R})$ is id: for $x \geq 0$, one has $x = y^2$ so that $\sigma(x) = \sigma(y)^2 \geq 0$, hence σ is non-decreasing, but $\sigma(q) = q$ for all $q \in \mathbb{Q}$ implies $\sigma(r) = r$ for all $r \in \mathbb{R}$.

Lemma 31.4: If F is a field extension of E, and K is an *intermediate field* (i.e. $E \subset K \subset F$), then $H = Aut_K(F)$ is a subgroup of $Aut_E(F)$; if $K_1 \subset K_2$ then $H_2 \leq H_1$ (of course, $Aut_F(F) = \{id\}$).
Proof: If $\sigma \in Aut(F)$ is the identity when restricted to K, then it is the identity when restricted to the smaller field E, and the larger the field the smaller the set of automorphisms which fix it, which is a group for composition.

Definition 31.5: If F is a field extension of E, and $X \subset Aut_E(F)$, then $Fix(X) = \{f \in F \mid \sigma(f) = f \text{ for all } \sigma \in X\}$.

Lemma 31.6: If F is a field extension of E, and $X \subset Aut_E(F)$, $Fix(X) = Fix(\langle X \rangle)$ is an intermediate field. If $H_1 \leq H_2 \leq Aut_E(F)$, then $Fix(H_2)$ is a subfield of $Fix(H_1)$.
Proof: If $X_1 \subset X_2 \subset Aut_E(F)$, one obviously has $Fix(X_2) \subset Fix(X_1)$. If $f \in Fix(X)$ and $\sigma \in X$, one has $\sigma(f) = f$, from which one deduces $\sigma^k(f) = f$ for $k \geq 1$, but one also has $\sigma^{-1}(f) = f$, so that $\sigma^n(f) = f$ for all $n \in \mathbb{Z}$; since each $\tau \in \langle X \rangle$ has the form $\tau = \sigma_1^{n_1} \cdots \sigma_k^{n_k}$ with $\sigma_1, \ldots, \sigma_k \in X$ and $n_1, \ldots, n_k \in \mathbb{Z}$, one deduces that $\tau(f) = f$, so that $Fix(X) \subset Fix(\langle X \rangle)$.

If $f_1, f_2 \in Fix(X)$, then for all $\sigma \in X$ one has $\sigma(f_1 + f_2) = \sigma(f_1) + \sigma(f_2) = f_1 + f_2$, so that $f_1 + f_2 \in Fix(X)$, and $\sigma(-f_1) = \sigma(-1)\,\sigma(f_1) = -f_1$, so that $-f_1 \in Fix(X)$, showing that $Fix(X)$ is a subgroup of F. Then, $\sigma(f_1 f_2) = \sigma(f_1)\,\sigma(f_2) = f_1 f_2$ so that $f_1 f_2 \in Fix(X)$, showing that $Fix(X)$ is a subring of F. Finally, if $f_1 \neq 0$, one has $1 = \sigma(1) = \sigma(f_1 f_1^{-1}) = \sigma(f_1)\,\sigma(f_1^{-1}) = f_1 \sigma(f_1^{-1})$, so that $\sigma(f_1^{-1}) = f_1^{-1}$, and $f_1^{-1} \in Fix(X)$, showing that $Fix(X)$ is a subfield of F.

Lemma 31.7: Let F be a field extension of E. If $H \leq Aut_E(F)$ and $K = Fix(H)$, then $H \leq Aut_K(F)$. If K' is an intermediate field, and $H' = Aut_{K'}(F)$, then $K' \subset Fix(H')$.
Proof: Immediate, since $h(k) = k$ for all $h \in H, k \in K$ in the first case, and for all $h \in H', k \in K'$ in the second case.

Remark 31.8: One then has a correspondence between intermediate fields (between E and its extension F) and subgroups of $Aut_E(F)$, and it is natural to wonder if this correspondence is a bijection. If $H = \{id\}$ then $Fix(H) = F$, but it is not always true that for $H = Aut_E(F)$ one has $Fix(H) = E$, hence the definition of a Galois extension (Definition 31.2) when it is true (and the extension is finite). It will be shown when the correspondence is a bijection, and the case where H is a normal subgroup of $Aut_E(F)$ will play a role.

Remark 31.9: If F is a field extension of E, then $a \in F$ is said to be algebraic over E if there exists a non-zero $P \in E[x]$ such that $P(a) = 0$, and then the ideal of polynomials $Q \in E[x]$ such that $Q(a) = 0$ is principal (since $E[x]$ is a PID) and generated by a monic polynomial of minimum degree, necessarily then irreducible, P_a called the minimal polynomial of a. The extension F of E is called algebraic if every element of F is algebraic over E, and a finite extension is necessarily algebraic.

Definition 31.10: A field extension F of E is called *normal* if and only if it is an algebraic extension, and for each $a \in F$ the associated monic irreducible polynomial P_a splits over F.

Remark 31.11: The reason for using the qualifier normal in Definition 31.10 will appear later, that if K is an intermediate field, then it is a normal extension of E if and only if $Aut_K(F)$ is a normal subgroup of $Aut_E(F)$.

Before stating the main theorems in Galois theory, another notion has to be introduced, separability, which is important in characteristic p (i.e. it automatically holds in characteristic 0); it is related to the fact that a non-constant polynomial P may satisfy $P' = 0$,[1] so that P has multiple roots.

[1] It happens if $P(x) = Q(x^p)$, which is not a statement about the value of P for some $x \in E$, but an abuse of notation, for $P = Q \circ \varphi_p$, where φ_p is the polynomial usually written x^p, whose only non-zero coefficient, equal to 1, is that of x^p.