Dec. 15, 2006

3.10. **solving cubic polynomials.** In this section, we are going to review classical result on solving polynomials by using non-classical language. I think this experience also serve a good start for Galois theory in general.

Definition 3.10.1. *A* **character** *from a group G to a field K is group homomorphism $\chi : G \to K^*$. The set of characters is denoted $Hom_{gp}(G, K^*)$.*

Let $Hom(G, K)$ be the set of functions from G to K. It's clear that $Hom(G, K)$ is a K-vector space.

Theorem 3.10.2 (E. Artin)**.** *$Hom_{gp}(G, K^*)$ is linearly independent in $Hom(G, K)$.*

Proof. Suppose on the contrary that $Hom_{gp}(G, K^*)$ is not linearly independent. Pick a linearly dependent subset $\{\chi_1, ..., \chi_n\}$ of minimal n. There are $a_i \in K$ such that $\sum a_i\chi_i = 0$, i.e.

$$\sum a_i\chi_i(g) = 0, \tag{$*$}$$

for all $g \in G$. We can rewrite it as

$$\sum a_i\chi_i(gh) = 0, \tag{$**$}$$

for all $g, h \in G$. Multiply $(*)$ by $\chi_1(h)$, we get

$$\sum a_i\chi_i(g)\chi_1(h) = 0. \tag{$***$}$$

Compare $(*)$ with $(***)$, we get

$$\sum a_i(\chi_i(h) - \chi_1(h))\chi_i(g) = 0 \text{ for all } g \in G.$$

Thus $\sum_{i=2}^{n} a_i(\chi_i(h) - \chi_1(h))\chi_i = 0 \in Hom(G, K)$. It follows that the $n - 1$ elements $\{\chi_2, ..., \chi_n\}$ is linearly dependent, which is a contradiction to the minimality. □

Corollary 3.10.3. *Let F/K be an extension. The set of K-homomorphisms from F to $\overline{K}$ is linearly independent in the $\overline{K}$-vector space of linear maps from F to $\overline{K}$.*

Sketch. Take $G = F^*$. □

Let K be a field containing n-th root of unity ζ. Let F/K be a Galois extension with Galois group $\cong \mathbb{Z}_n$ generated by σ. We consider

$$\psi_\zeta := 1 + \zeta\sigma + \zeta^2\sigma^2 + ... + \zeta^{n-1}\sigma^{n-1} \in Hom(F, \overline{K}).$$

Any element of the form $\psi(x)$ is called a **Lagrange resolvent**.

By direct computation, we have the following properties.

Proposition 3.10.4. *Keep the notation as above, we have:*
1. $\sigma(\psi_\zeta(x)) = \zeta^{-1}\psi_\zeta(x)$.
2. $\psi_1(x) \in K$.
3. $(\psi_\zeta(x))^n \in K$.
4. $(\psi_\zeta(x))(\psi_{\zeta^{-1}}(x)) \in K$.
5. $\sum_{\zeta\in\mu_n} \zeta^{-r}\psi_\zeta(x) = n\sigma^r(x)$.

Now we can use this technique to solve cubic equations. Let $f(x) = x^3 + px + q \in K[x]$ be an irreducible polynomial with discriminant $D = -4p^3 - 27q^2 \in K$. We assume that K contains a primitive 3-root of unity ζ. We have extension $K \subset L := K[\sqrt{D}] \subset F := K[u_1, u_2, u_3]$. Note that F/L is Galois with Galois group $\cong \mathbb{Z}_3$.
Step 1. $\psi_\zeta \neq 0 \in Hom(F, \overline{K})$, in fact $\psi_\zeta(u_1) \neq 0$.

Step 2. $\psi_\zeta(u_1) \neq L$ and $(\psi_\zeta(u_1))^3 \in L$, thus $F = L[\psi_\zeta(u_1)]$.
And similarly, $\psi_{\zeta^2}(u_1) \in L, (\psi_{\zeta^2}(u_1))^3 \in L$. Moreover, $\psi_\zeta(u_1)\psi_{\zeta^2}(u_1) \in L$.
Step 3. Solve $\psi_\zeta(u_1)$,$\psi_{\zeta^2}(u_1)$.
Recall that

$$\Delta := (u_1-u_2)(u_2-u_3)(u_3-u_1) = u_1^2u_2+u_2^3u_3+u_3^2u_1-u_1u_2^2-u_2u_3^2-u_3u_1^2.$$

$$\psi_\zeta(u_1)^3 = u_1^3+u_2^3+u_3^3+3\zeta(u_1^2u_2+u_2^2u_3+u_3^2u_1)+\zeta^2(u_1u_2^2+u_2u_3^2+u_3u_1^2)+6u_1u_2u_3.$$

Let $v_1 = u_1^2u_2 + u_2^2u_3 + u_3^2u_1, v_2 = u_1u_2^2 + u_2u_3^2 + u_3u_1^2$, then

$$v_1 + v_2 = (u_1 + u_2 + u_3)(u_1u_2 + u_2u_3 + u_3u_1) - 3u_1u_2u_3 = 3q,$$

$$v_1 - v_2 = \Delta.$$

Thus $\psi_\zeta(u_1)^3$ can be expressed in terms of p, q, Δ.
Step 4. solve u_1, u_2, u_3 in terms of $\psi_\zeta(u_1)$,$\psi_{\zeta^2}(u_1)$.
By the property 5 above, we have

$$3u_1 = \psi_1(u_1) + \psi_\zeta(u_1) + \psi_{\zeta^2}(u_1),$$

$$3u_2 = 3\sigma(u_1) = \psi_1(u_1) + \zeta^{-1}\psi_\zeta(u_1) + \zeta^{-2}\psi_{\zeta^2}(u_1),$$

$$3u_3 = 3\sigma^2(u_1) = \psi_1(u_1) + \zeta^{-2}\psi_\zeta(u_1) + \zeta^{-1}\psi_{\zeta^2}(u_1).$$

And note that $\psi_1(u_1) = 0$. So one can solve cubic polynomial explicitly.

3.11. **cyclic extension.** The discussion in the previous section can be extended to a more general setting.

Definition 3.11.1. *We say that an extension is cyclic (resp. abelian) if it's algebraic Galois and* $\mathrm{Gal}_{F/K}$ *is cyclic (resp. abelian). An cyclic extension of order n is an cyclic extension whose Galois group is isomorphic to $\mathbb{Z}_n$.*

The following theorem characterize cyclic extension except some exceptional case.

Theorem 3.11.2. *Suppose that* $char(K) = 0$ *or* $char(K) = p \nmid n$. *Suppose furthermore that there is a primitive* n*-th root of unity in* K, *say* ζ. *Then* F/K *is a cyclic of order* n *if and only if* $F = K(u)$ *where* u *is a root of irreducible polynomial* $x^n - a \in K[x]$.

Before we get into the proof. Let's consider the "difference" between u and $\sigma(u)$ for $\sigma \in \mathrm{Gal}_{F/K}$. Let F/K be a finite Galois extension. Then in this circumstance, norm and trace (which we will define more generally later) are nothing but $N_{F/K}(u) := \prod_{\sigma \in \mathrm{Gal}_{F/K}} \sigma(u)$ and $T_{F/K} := \sum_{\sigma \in \mathrm{Gal}_{F/K}} \sigma(u)$. It's easy to see that $T(u - \sigma(u)) = 0$ and $N(u/\sigma(u)) = 1$. The follows lemma says that the converse is also true for cyclic extension, which will play the central role in the study of cyclic extension.

Lemma 3.11.3. *Let* F/K *be an cyclic extension with* σ *the generator of the Galois group.*

(1) *If* $T_{F/K}(u) = 0$, *then there exists an* $v \in F$ *such that* $u = v - \sigma(v)$.
(2) *(Hilbert's Theorem 90) If* $N_{F/K}(u) = 1$, *then there exists an* $v \in F$ *such that* $u = v/\sigma(v)$.

Proof of the Theorem 3.11.2. Let u be a root of $x^n - a$, then all the roots are $u\zeta^i$ for $i = 0, ..., n-1$. Since $\zeta \in K$. We can produce an element in Galois group by considering $\sigma_i : u \mapsto u\zeta^i$. Thus we have $\{\sigma_i\}_{i=0,\ldots,n-1} \subset \mathrm{Gal}_K F$. It's clear that $\mathrm{Gal}_K F = \{\sigma_i\}_{i=0,\ldots,n-1} =< \sigma_1 >$. Thus $F = K(u)$ is a cyclic extension over K.

Conversely, suppose that F/K is a cyclic extension of order n. Since there is a primitive n-th root $\zeta \in K$, one has $N(\zeta) = \zeta^n = 1$. By the Lemma, there exist an v such that $\zeta = v/\sigma(v)$. Let $u = v^{-1}$, then $\sigma(u) = \zeta u$. Hence $\sigma(u^n) = u^n \in K$. Therefore u satisfies $x^n - a \in K[x]$ for some $a \in K$.

Moreover, for $u\zeta^i$ and $u\zeta^j$, there is an automorphism sending $u\zeta^i$ to $u\zeta^j$. So they have the same minimal polynomial $p(x)$ dividing $x^n - a$. One the other hand, $p(x)$ has n distinct roots $u\zeta^i$ for $i = 0, ..., n-1$. It follows that $p(x) = x^n - a$ is irreducible. One has $[K(u) : K] = n$ and thus $F = K(u)$. □

Theorem 3.11.4. *Suppose that* $char(K) = p \neq 0$. *Then* F/K *is a cyclic extension of order* n *if and only if* $F = K(u)$, *where* u *is a root of an irreducible polynomial* $x^p - x - a \in K[x]$.

Proof. The proof is parallel to the previous one.

Let u be a root of $x^p - x - a$, then all the roots are $u + i$ for $i = 0, ..., p-1$. It's clear that $F = K(\zeta)$ is a cyclic extension over K with Galois group generated by σ such that $\sigma(u) = u + 1$.

Conversely, suppose that F/K is a cyclic extension of order n. One has $T(1) = p = 0$. By the Lemma, there exist an v such that $1 =$

$v - \sigma(v)$. Let $u = -v$, then $\sigma(u) = u + 1$. Hence $\sigma(u^p) = u^p + 1$ and $\sigma(u^p - u) = u^p - u$. Therefore u satisfies $x^p - x - a \in K[x]$ for some $a \in K$.

Moreover, for $u + i$ and $u + j$, there is an automorphism sending $u\zeta^i$ to $u\zeta^j$. So they have the same minimal polynomial $p(x)$ dividing $x^p - x - a$. One the other hand, $p(x)$ has p distinct roots $u + i$ for $i = 0, ..., p - 1$. It follows that $p(x) = x^p - x - a$ is irreducible. One has $[K(u) : K] = n$ and thus $F = K(u)$. □

It remains to define norm and trace, and prove the main lemma 3.11.3.

Definition 3.11.5. *Let $[F : K]$ be a finite separable extension. Let Σ be the set of K-embeddings of F into $\overline{K}$. For any $u \in F$, we define the norm, denoted*

$$N_{F/K}(u) := (\prod_{\sigma\in\Sigma} \sigma(u)).$$

Similarly, we define the trace as

$$T_{F/K}(u) := (\Sigma_{\sigma\in\Sigma}\sigma(u)).$$

Example 3.11.6. *If F/K is finite Galois extension, then the set of all K-embeddings of F is nothing but the Galois group of F (since F is normal). Therefore, $N_{F/K}(u) = \prod_{\sigma\in\mathrm{Gal}_{F/K}} \sigma(u)$ and $T_{F/K}(u) = \sum_{\sigma\in\mathrm{Gal}_{F/K}} \sigma(u)$*

Proof of Lemma 3.11.3. We only prove that $T(u) = 0$ implies $u = v - \sigma(v)$. The other implication is easy.

Step 1. Find an element $z \in F$ with $T(z) \neq 0$. This is an immediate consequence of independency of automorphism.

Step 2. We normalize it to get $w \in F$ with $T(w) = 1$. In fact, we take $w := \frac{z}{T(z)}$.

Step 3. Let

$$v = uw + (u + \sigma(u))\sigma(w) + ... + (u + \sigma(u) + ... + \sigma^{n-2}(u))\sigma^{n-2}(w).$$

Then by direct computation and $T(u) = \sum \sigma(u) = 0$, we are done.

For the norm, if $N(u) = 1$, then $u \neq 0$. Take

$$v = uy + u\sigma(u)\sigma(y) + ... + u\sigma(u)...\sigma^{n-1}(u)\sigma^{n-1}(y).$$

By independency of automorphism, there exist a y such that v is non-zero. One checks that $u^{-1}v = \sigma(v)$. We are done. □

3.12. radical extension.

Definition 3.12.1. *F/K is said to be an radical extension if $F = K(u_1, ..., u_n)$ such that for $1 \leq i \leq n$, $u_i^{n_i} \in K(u_1, ..., u_{n-1})$.*

For a polynomial $f(x) \in K[x]$. We say $f(x) = 0$ is solvable by radical if its splitting field E is contained in some radical extension.

Remark 3.12.2. *In the definition, it's not necessary that the splitting field itself is a radical extension over K.*

The main observation is the following:

Proposition 3.12.3. *Let F/K be a radical and Galois extension over K. Write $F = K(u_1, ..., u_n)$ such that for $1 \le i \le n$, $u_i^{n_i} \in K(u_1, ..., u_{n-1})$. Let $m = \prod n_i$ and assume that $char(K) \nmid m$. Suppose furthermore that K contains a primitive m-th root of unity. Then $\mathrm{Gal}_{F/K}$ is solvable.*

Proof. Let $K_i := K(u_1, ..., u_i)$. And let $G_i = K_i'$. One sees that K_1 is cyclic over K, hence Galois over K. Hence $G_1 \lhd G_0 = \mathrm{Gal}_{F/K}$. Consider next F/K_1 which is radical and Galois. Then K_2 is cyclic over K_1 and hence similarly, $G_2 \lhd G_1$. Therefore, we have a solvable series $\{e\} = G_n \lhd G_{n-1} \lhd ... \lhd G_0 = \mathrm{Gal}_{F/K}$ with G_{i-1}/G_i cyclic. We are done. □

One can actually generalize it to the following general setting:

Theorem 3.12.4. *Let F/K be a radical extension, and $K \subset E \subset F$. Then $\mathrm{Gal}_{E/K}$ is solvable. As a consequence, if $f(x) = 0$ is solvable by radical, then G_f is solvable.*

Proof. We first reduce to simpler situation.
Step 1. Let $G = \mathrm{Gal}_{E/K}$ and $K_0 = G'$. It's clear that F/K_0 is radical, and E/K_0 is Galois for $\mathrm{Gal}_{E/K_0} = G'' = G$ and $G''' = G'$. Thus F/K_0 is radical and E/K_0 is Galois with Galois group $\mathrm{Gal}_{E/K}$.

We thus replacing K by K_0 and assume that E/K is Galois.
Step 2. Reduce to the case that $E = F/K$ is Galois. To see this, let $\sigma : F \to \overline{K}$ be an K-embedding. One can show that $\sigma(F)$ is again a radical extension. One can also prove that if $F_1, F_2 \subset \overline{K}$ are radical extension over K, then F_1F_2 is a radical extension over K. Hence let N be the compositum of $\sigma(F)$ for all σ. It follows that N is radical over K. Moreover, N is normal over K.

Since E/K is Galois, in particular, E is normal over K and E is a stable intermediate subfield of N/K. Then one has a homomorphism $\mathrm{Gal}_{N/K} \to \mathrm{Gal}_{E/K}$. This is surjective because N is normal. Thus it suffices to prove that $\mathrm{Gal}_{N/K}$ is solvable.
Step 3. By the same trick an in Step 1. We may assume that N/K is Galois. Therefore, it suffices to show that if F/K is Galois and radical, then $\mathrm{Gal}_{F/K}$ is solvable.
Step 4. Since F/K is separable, we may assume that $(\mathrm{char}(K), n_i) = 1$. Let $m = \prod n_i$.

Let ζ be a primitive m-th root of unity. We claim that $F(\zeta)$ is Galois over K. Grant this for the time being, then $F(\zeta)$ is Galois over $K(\zeta)$ and $K(\zeta)' \lhd \mathrm{Gal}_{F(\zeta)/K}$. Moreover, $\mathrm{Gal}_{F(\zeta)/K}/K(\zeta)' \cong \mathrm{Gal}_{K(\zeta)/K}$. By Proposition 3.12.3, $K(\zeta)'$ is solvable. $K(\zeta)/K$ is cyclotomic, hence $\mathrm{Gal}_{K(\zeta)/K}$ is solvable. Thus, $\mathrm{Gal}_{F(\zeta)/K}$ is solvable.

Now F/K is Galois, $\mathrm{Gal}_{F/K} \cong \mathrm{Gal}_{F(\zeta)/K}/F'$ which is solvable.

Step 5. To prove the claim, suppose that F is a splitting field of separable polynomial $f_1, .., f_n \in K[x]$. Then $F(\zeta)$ is nothing but a splitting field of separable polynomials $f_1, ..., f_n, x^m - 1$. Thus we are done. $\square$

Theorem 3.12.5. *Let E be a finite dimensional Galois extension over K with solvable Galois group. Assume that $char(K) \nmid [E : K]$, then there is a radical extension F/K containing E.*

Proof. We prover by induction on $[E : K]$. Let $n = [E : K]$ and assume the theorem is true for all Galois extension of degree $< n$.

Let ζ be a primitive n-th root of unity. Then $E(\zeta)/K(\zeta)$ is Galois. If $[E(\zeta) : K(\zeta)] < n$ then we are done by induction hypothesis and the fact that $K(\zeta)/K$ is radical.

By replacing E, K by $E(\zeta), K(\zeta)$ respectively, we my assume that K has m-th root of unity.

$\mathrm{Gal}_{E/K}$ is solvable, let H be a subgroup of index q, for some prime q. Then H'/K is a cyclic extension, hence a radical extension. By induction hypothesis, E/H' is radical. We are done. $\square$

Corollary 3.12.6. *Let $f(x) \in K[x]$ be a polynomial of degree $n > 0$. Suppose that $char(K) \nmid n!$, then $f(x) = 0$ is solvable by radical if and only if G_f is solvable.*