Dec. 1, 2006

Remark 3.6.8. *Some of the result we proved still true in a more general setting. We list some here:*

1. *If F/K is an extension, and an intermediate field E is stable, then $E' \lhd \mathrm{Gal}_{F/K}$.*
2. *Let F/K be an extension. If $N \lhd \mathrm{Gal}_{F/K}$, then H' is stable.*
3. *If F/K is Galois, and E is a stable intermediate field, then E is Galois over K. (finite-dimensional assumption is unnecessary here)*
4. *An intermediate field E is algebraic and Galois over K, then E is stable.*

We conclude this section with the following theorem concerning the relation between Galois extension, normal extension and splitting fields.

Definition 3.6.9. *An irreducible polynomial $f(x) \in K[x]$ is said to be* **separable** *if its roots are all distinct in $\overline{K}$.*

Let F be an extension over K and $u \in F$ is algebraic over K. Then u is separable over K if its minimal polynomial is separable.

An extesnion F over K is separable if every element of F is separable over K.

Theorem 3.6.10. *Let F/K be an extension, then the following are equivalent*

1. *F is algebraic and Galois over K.*
2. *F is separable over K and F is a splitting field over K of a set S of polynomials.*
3. *F is a splitting field of separable polynomials in $K[X]$.*
4. *F/K is normal and separable.*

Proof. Fix $u \in F$ with minimal polynomail $p(x)$ over K. Let $\{u = u_1, ..., u_r\}$ be distinct roots of $p(x)$ in F. For any σ, then σ permutes $\{u = u_1, ..., u_r\}$. Thus $f(x) := \prod_{i=1}^{r}(x - u_i)$ is invariant under σ. Hence $f(x) \in K[x]$. It follows that $f(x) = p(x)$. This proved that $(1) \Rightarrow (2), (3), (4)$.

One notices that $(2) \Leftrightarrow (4)$. Thus it remains to show that $(2) \Rightarrow (3)$, and $(3) \Rightarrow (1)$.

For $(2) \Rightarrow (3)$, let $f(x) \in S$ and let $g(x)$ be an monic irreducible component of $f(x)$. Since $f(x)$ splits in F, it's clear that $g(x)$ is an minimal polynomial of some element in F. Moreover, since F/K is separable, $g(x)$ is separable. One sees that F is in fact a splitting field of such $g(x)$'s.

For $(3) \Rightarrow (1)$, we first note that F/K is algebraic since F is a splitting field. We shall prove that $(4) \Rightarrow (1)$. The implication $(3) \rightarrow (4)$ follows from a general fact about separable extension that an algebraic extension F/K is separable if F is generated by separable elements.

To this end, pick any $u \in F - K$, with minimal polynomial $p(x)$ of degree ≥ 2 and separable. Hence there is a different root, say v, of $p(x)$ in F. It's natural to consider the K-isomorphism $\sigma : K(u) \to K(v)$. Which can be extended to $\bar{\sigma} : F \to \overline{K}$. Since F is normal, $\bar{\sigma}$ is an automorphism of F, hence in $\mathrm{Gal}_{F/K}$ sending u to $v \neq u$. So F/K is Galois.

□

3.7. **Galois group of a polynomial.** In this section, we are going to study Galois group of a polynomial. We will define this notion in general and study polynomial of degree 3,4 in more detail.

Definition 3.7.1. *Let $f \in K[x]$ be a polynomial with splitting field F. The Galois group of $f(x)$, denoted G_f is the Galois group of F/K.*

The Galois group of a polynomial have some basic properties.

Proposition 3.7.2. *Let $f(x)$ be a polynomial of degree n, then $G_f \hookrightarrow S_n$. Thus one can viewed G_f as a subgroup of S_n.*

If $f(x)$ is irreducible and separable, then G_f is transitive and $|G_f|$ is divided by n.

Sketch of the proof. Let $\{u_1, ..., u_r\}$ be roots of $f(x)$ in F. For $\sigma \in G_f$, $\sigma(u_i) = u_j$. Hence σ gives a permutation of r elements. It follows that G_f can be viewed as a subgroup of S_r hence S_n.

(r could possibly less than n because there might have multiple roots in general).

Now if $f(x)$ is separable. Then we have distinct roots $\{u_1, ..., u_n\}$ in F. For any u_i, we have $K[u_i] \cong K[x]/(f(x))$ since $f(x)$ is irreducible. If follows that there is a K-isomorphism $\sigma : K[u_i] \to K[x]/(f(x)) \to K[u_j]$ for all i, j. *sigma* gives an K-embedding $K[u_i] \to \overline{K[u_j]} = \overline{K}$ and extended to a K-embedding $\bar{\sigma} : F \to \overline{K}$. Since F is normal, $\bar{\sigma}(F) = F$ (cf. Theorem ?). Thus $\bar{\sigma} \in G_f$ and $\bar{\sigma}(u_i) = \sigma(u_i) = u_j$. Therefore, G_f is transitive.

Moreover, since $K \subset K[u_i] \subset F$. So $|G_f| = [F : K] = [F : K[u_i]]n$ is divided by n. □

So now, we discuss irreducible separable polynomials of small degree. One might wondering how do we know a polynomial is separable or not. We have the following easy criteria:

Proposition 3.7.3. *Let $f(x) \in K[x]$ be an irreducible polynomial The following are equivalent:*

1. *$f(x)$ is separable.*
2. *$(f(x), f'(x)) = 1$ in $\overline{K}[x]$*
3. *$(f(x), f'(x)) = 1$ in $K[x]$*
4. *$f'(x) \neq 0$*

Recall that when $f(x) = \sum a_i x^i$, then $f'(x)$ is its formal differentiation which is $f'(x) := \sum i a_i x^{i-1}$.

Proof. If $f(x)$ is separable, then $f(x) = \prod_{i=1}^{n}(x - u_i)$ with distinct u_i in $\overline{K}[x]$. Thus $f'(x) = \sum \frac{\prod_{i=1}^{n}(x-u_i)}{x-u_i}$. If $(f(x), f'(x)) \neq 1$ in $\overline{K}[x]$, then $x - u_i | f'(x)$ for some i. However, $f'(u_i) = \prod_{j \neq i}(u_j - u_i) \neq 0$, a contradiction.

Conversely, if $f(x)$ is not separable, then $f(x) = \prod_{i=1}^{r}(x - u_i)^{a_i}$ with some $a_i \geq 2$. Let's say $a_1 \geq 2$. Then it's clear that $(x - u_1)$ is a factor of $f'(x)$ as well. Hence $(f(x), f'(x)) \neq 1$. This proved the equivalence of (1) and (2).

To see the equivalence of (2) and (3). Note that if $(f(x), f'(x)) = 1$ in $K[x]$, then $1 = f(x)s(x) + f'(x)t(x)$ for some $s(x), t(x) \in K[x]$. One can view this in $\overline{K}[x]$ and thus conclude that $(f(x), f'(x)) = 1$ in $\overline{K}[x]$. On the other hand, if $(f(x), f'(x)) = d(x) \neq 1$ in $K[x]$, then $d(x) = f(x)s(x) + f'(x)t(x)$ for some $s(x), t(x) \in K[x]$. One can view this in $\overline{K}[x]$ and thus conclude that $d(x)|(f(x), f'(x))$ in $\overline{K}[x]$. In particular, $(f(x), f'(x)) \neq 1$ in $\overline{K}[x]$

Now finally, since $f(x)$ is irreducible, $(f(x), f'(x))$ could only be 1 or $f(x)$. Since $f(x)|f'(x)$ if and only $f'(x) = 0$. Thus we are done. □

One notice that if $\mathrm{char} K \neq 0$, then an irreducible polynomial is always separable. When $\mathrm{char} K = p$, then an irreducible polynomial $f(x)$ is not separable if and only $f(x) = g(x^p)$ for some $g(x)$.

One can go a little bit further. If K is finite field with $\mathrm{char} K = p$. Let $f(x) = \sum a_i x^i$ be an irreducible polynomial. $f'(x) = 0$ means that $p|i$ for all $a_i \neq 0$. Thus $f(x)$ can be rewrite as $\sum a_i x^{ip}$. Recall that each a_i can be written as b_i^p for some b_i because K is finite. Thus $f(x) = \sum b_i^p x^{ip} = (\sum b_i x^i)^p$. This contradicts to $f(x)$ being irreducible. To sum up, an irreducible polynomial over a finite field is always separable.

Let's now turn back to the discussion of Galois groups. If $f(x)$ is irreducible and separable of degree 2, then $G_f \cong S_2 \cong \mathbb{Z}_2$. If $f(x)$ is irreducible and separable of degree 3, then G_f is a subgroup of S_3 of order divided by 3. Thus G_f could be A_3 or S_3. The question now is how to distinguish these two cases.

Lemma 3.7.4. ($\mathrm{char} K \neq 2$) *Let $f(x) \in K[x]$ be an irreducible and separable polynomial of degree 3 with splitting field F and roots u_1, u_2, u_3. Then $(G_f \cap A_3) = K[\Delta]$, where $\Delta := (u_1 - u_2)(u_1 - u_3)(u_2 - u_3)$*

Note that $f(x)$ is irreducible and separable, then F/K is Galois. And Δ^2 is invariant under G_f. Thus $D := \Delta^2 \in K$. We call D the discriminant of $f(x)$.

If $f(x)$ is written as $x^3 + bx^2 + cx + d$, then $s_1 := u_1 + u_2 + u_3 = -b$, $s_2 := u_1u_2 + u_1u_3 + u_2u_3 = c$, $s_3 := u_1u_2u_3 = -d$. We impose an ordering $u_1 > u_2 > u_3$. Then leading term of D is $u_1^4u_2^2$, which is the leading term of $s_1^2s_2^2$. Then we consider $D' := D - s_1^2s_2^2$ with lower leading term, which is $-4u_1^3u_2^3$. This leading term is the same as the leading term of $-4s_2^3$. So we consider $D^{(2)} := D' + 4s_2^3$. Inductively, one can write D in terms of s_1, s_2, s_3, hence in terms of b, c, d.

If $f(x)$ is normalized as $x^3 + px + q$, then $D = -4p^3 - 27q^2$.

Proof. $\sigma(\Delta) = \Delta$ if and only σ is an even permutation. So $\Delta \in (G_f \cap A_3)'$ clearly. Hence we have $K[\Delta] < (G_f \cap A_3)'$. Thus $K[\Delta]' > (G_f \cap A_3)$. If $\sigma \in K[\Delta]'$, then $\sigma(\Delta) = \Delta$, hence σ is even. Thus $K[\Delta]' < (G_f \cap A_3)$. So we have $K[\Delta]' = (G_f \cap A_3)$ and $K[\Delta] = (G_f \cap A_3)'$. $\square$

We thus conclude that $G_f = A_3$ if and only if D_f is square in K. And $G_f = S_3$ if and only if D_f is not a square in K

Example 3.7.5.

Let $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$. It's irreducible.

Now we consider the case of degree 4 polynomial. One can also define Δ and discriminant D similarly. However, it turns out that this is not enough to classify all cases. The idea is to consider another normal subgroup $V_4 \lhd S_4$.

Let's first list at all possible subgroup in S_4. Since G_f is transitive with order divided by 4. We can have following

$\lvert G_f\rvert$	G_f	$G_f \cap V_4$	$\lvert G_f\rvert/\lvert G_f \cap V_4\rvert$
24	S_4	V_4	6
12	A_4	V_4	3
8	$\cong D_8$	V_4	2
4	$\cong \mathbb{Z}_4$	$\neq V_4$	2
4	V_4	V_4	1

Also we have the following

Lemma 3.7.6. *Let $f(x)$ be an irreducible separable polynomial of degree 4 with splitting field F and roots u_1, K, u_4. Let $\alpha = u_1u_2 + u_3u_4$ $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3$. Then $K[\alpha, \beta, \gamma] = (G_f \cap V_4)$.*

Let $g(x) = (x-\alpha)(x-\beta)(x-\gamma)$, then one can check that $\sigma(g(x) = g(x)$ for all $\sigma \in G_f$. Thus $g(x) \in K[x]$ for F/K is Galois. The cubic $g(x)$ is call the **resolvant cubic** of $f(x)$. If $f(x) = x^4+bx^3+cx^2+dx+e$, then its resolvant cubic is $g(x) = x^3 - cx^2 + (bd-4e)x - b^2e + 4ce - d^2$ by computation on symmetric polynomials as we exhibited.

Proof. It clear that $K[\alpha, \beta, \gamma] < (G_f \cap V_4)'$. Hence we have $(G_f \cap V_4) < K[\alpha, \beta, \gamma]'$. Now if $\sigma \in K[\alpha, \beta, \gamma]'$ and $\sigma \ni V_4$. We claim that this would lead to a contradiction. And thus we are done.

The claim can be verified directly by exhausting all cases. For example, if $\sigma = (1, 3)$, then $\sigma(\alpha) = \alpha$ gives $u_3u_2 + u_1u_4 = u_1u_2 + u_3u_4$. Thus $(u_2 - u_4)(u_1 - u_3) = 0$ contradict to reparability of $f(x)$. The other cases can be computed similarly.

$\square$

Let $m := |G_f|/|G_f \cap V_4| = [K[\alpha, \beta, \gamma] : K]$. By using this correspondence, one sees that:
1. $m = 1 \Leftrightarrow G_f = V_4 \Leftrightarrow g(x)$ splits into linear factors in $K[x]$.
2. $m = 3 \Leftrightarrow G_f = A_4 \Leftrightarrow g(x)$ is irreducible in $K[x]$ and D_g is a square in K.
3. $m = 6 \Leftrightarrow G_f = S_4 \Leftrightarrow g(x)$ is irreducible in $K[x]$ and D_g is not a square in K.

The only remaining unclear case is $m = 2$. This case corresponding to the case that $g(x)$ splits into a linear and a quadratic factors in $K[x]$. To see the Galois group, we claim that $G_f \cong D_8$ if and only if $f(x)$ is irreducible in $K[\alpha, \beta, \gamma][x]$.

First of all, if $f(x)$ is irreducible in $K[\alpha, \beta, \gamma][x]$, then

$$4 = [K[\alpha, \beta, \gamma][u_1] : K[\alpha, \beta, \gamma]] \leq [F : K[\alpha, \beta, \gamma]] = |G_f \cap V_4|.$$

So $G_f \cong D_8$.

On the other hand, F is the splitting field of $f(x)$ over $K[\alpha, \beta, \gamma]$ as well. Suppose that $f(x)$ is reducible. If $f(x)$ factors into a linear and a cubic factor in $K[\alpha, \beta, \gamma]$, then the Galois group of $f(x)$ over $K[\alpha, \beta, \gamma]$, which is $G_f \cap V_4$, can only $\cong A_3$ or S_3. This is a contradiction. Running over all cases, one sees that the only possible case is $f(x)$ factors into two linear and one quadratic factors. Thus $|G_f \cap V_4| = 2$ and hence $G_f \cong \mathbb{Z}_4$.

3.8. **finite fields.** The Galois theory on finite fields is comparatively easy and basically governed by Frobenius map.

Recall that given a finite field F of q elements, it's prime field must be of the form $\mathbb{F}_p$ for some prime p. Let $n = [F : \mathbb{F}_p]$, then $|F| = p^n$.

Theorem 3.8.1. *F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_n$.*