Dec. 8, 2006

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 $\mathbb{F}_p$.*

Sketch. Recall that F^* is a multiplicative group of order $p^n - 1$. Hence it's easy to see that every element $u \in F$ satisfying $x^{p^n} - x$. Thus element of F are exactly roots of $x^{p^n} - x$, therefore, F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Conversely, if F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $E \subset F$ be the subset of all roots of $x^{p^n} - x$. One can check that E is a subfield (containing $\mathbb{F}_p$ and all roots). By definition of splitting field, E is a splitting field, and $E = F$. So $|F| = |E| \leq p^n$. However, notice that $x^{p^n} - x$ is separable. So $|F| = p^n$. $\square$

Proposition 3.8.2. *Let F be a finite field and F/K is an extension. Then F/K is Galois. The Galois group is cyclic, generated by Frobenius map.*

Proof. We shall prove the case that $K = \mathbb{F}_p$. For general K, $\mathbb{F}_p \subset K \subset F$. Since $F/\mathbb{F}_p$ is Galois, then F/K is also Galois with Galois group $K' < \mathrm{Gal}_{\mathbb{F}_p} F$ also a cyclic group.

Now we consider $F/\mathbb{F}_p$, and $|F| = p^n$. Since F is a splitting field of a separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$, F is Galois over $\mathbb{F}_p$.

The Galois group $\mathrm{Gal}_{\mathbb{F}_p} F$ has order $[F : \mathbb{F}_p] = n$. Consider the Frobenius map $\varphi : a \to a^p$, which is clearly a $\mathbb{F}_p$-automorphism. So $\varphi \in \mathrm{Gal}_{\mathbb{F}_p} F$. Note that order of φ is n. So $\mathrm{Gal}_{\mathbb{F}_p} F$ can only be the cyclic group generated by φ. $\square$

3.9. **cyclotomic extension.** We now start the study of cyclotomic extension.

Definition 3.9.1. *A cyclotomic extension of order n over K is a splitting field of $x^n - 1$.*

Remark 3.9.2. *If $char(K) = p$ and $n = p^r m$, then $x^n - 1 = (x^m - 1)^{p^r}$. Hence we may assume that either $char(K) = 0$ or $char(K) = p \nmid n$ in the study of cyclotomic extension.*

The main theorem is the following:

Theorem 3.9.3. *Keep the notation as above. Then we have*

1. *$F = K(\zeta)$, where ζ is a primitive n-th root of unity.*
2. *F/K is Galois whose Galois group $\mathrm{Gal}_{F/K}$ can be identified as a subgroup of $\mathbb{Z}_n^*$.*

(3) *If n is prime, then $\mathrm{Gal}_{F/K}$ is cyclic. More general, is $n = p^k$ with $p \neq 2$, then then $\mathrm{Gal}_{F/K}$ is cyclic.*

Proof. Let $S := \{u \in F | u^n = 1\}$. And let n' be the maximal order of elements in S. Clearly, $n' \leq n$ It's clear that S is an abelian multiplicative group. Therefore, it's easy to see that order of elements in S divides n'. It follows that $u^{n'} = 1$ for all $u \in S$. Hence $|S| \leq n'$.

Since we assume that $(n, \mathrm{char}(K)) = 1$, therefore $x^n - 1$ is separable. It follows that roots of $x^n - 1$ are all distinct, hence $|S| = n$. One sees that $n = n'$, therefore, there are elements of order n in S, denoted ζ. It follows that $F = K(S) = K(\zeta)$.

For any $\sigma \in \mathrm{Gal}_{F/K}$, $\sigma(\zeta) \in S$. Hence $\sigma(\zeta) = \zeta^i$ for some i. Therefore, we have a natural map $\phi : \mathrm{Gal}_{F/K} \to \mathbb{Z}_n$ by $\phi(\sigma) = i$ if $\sigma(\zeta) = \zeta^i$. Note that if ζ^i is not a primitive n-th root of unity, then $K(\zeta^i)$ is not the splitting field of $x^n - 1$, hence not equal to $K(\zeta)$, which is absurd. Thus sigma we conclude that ζ^i is a primitive n-th root of unity. It's easy to see that this is equivalent to $(i, n) = 1$. Thus $\phi : \mathrm{Gal}_{F/K} \to \mathbb{Z}_n^*$ is an injective group homomorphism.

Lastly, if $n = p^k$ with $p \neq 2$ or if $n = 2, 4$, then $\mathbb{Z}_n^*$ is cyclic. Hence every subgroup is cyclic. $\square$

The structure of cyclotomic extension is thus determined by the primitive n-th root of unity. It's then natural to ask the degree of such extension and their minimal polynomials.

Definition 3.9.4. *If $\mathrm{char} K \nmid n$, then the n-th* **cyclotomic polynomial** *over K is defined as:*

$$g_n(x) := \prod_{\zeta_i\text{: prim. } n\text{-th root of 1}} (x - \zeta_i).$$

Proposition 3.9.5. *We have the following:*
1. $x^n - 1 = \prod_{d|n} g_d(x)$.
2. *$g_n(X) \in P[x]$, where P denoted the prime field. Moreover, if $\mathrm{char} K = 0$, we identify $P = \mathbb{Q}$, then $g_n(x) \in \mathbb{Z}[x]$.*
3. *$deg(g_n(x)) = \varphi(n)$, where φ denotes the Euler ϕ-function.*

Proof. (3) is clear from the definition.

For (1), we consider the following decomposition of sets

$$\{\zeta^i\}_{i=0,\ldots,n-1} = \cup_{d|n} \{\zeta^i | o(\zeta^i) = d\}.$$

Note that $o(\zeta^i) = d$ implies that ζ^i is a primitive d-th root of unity. Thus we define $g'_d(x) := \prod_{o(\zeta^i)=d}(x - \zeta^i)$, and then $g'_d(x) | g_d(x)$. By the decomposition, we have

$$x^n - 1 = \prod_{i=0,\ldots,n-1} (x - \zeta^i) = \prod_{d|n} g'_d(x).$$

Computing degrees, we have

$$n = \sum_{d|n} deg(g'_d(x)) \leq \sum_{d|n} deg(g_d(x)) = \sum_{d|n} \varphi(d) = n.$$

Therefore, $g'_d(x) = g_d(x)$.

To see (2), we prove by induction on n. We assume that $g_d(x) \in P[x]$ for all $d < n$. We can write $x^n - 1 = g_n(x)f(x) \in F[x]$. In $P[x]$, we have $x^n - 1 = f(x)q(x) + r(x)$ by the division algorithm. We shall prove that $r(x) = 0$ and thus $g_n(x) = q(x) \in P[x]$ by the unique factorization of $F[x]$.

It suffices to show that $r(x) = 0$. To this end, note that $f(x)|x^n - 1$ in $F[x]$, and thus $f(x)|r(x)$ in $F[x]$. However, $deg(r(x)) < deg(f(x))$ unless $r(x) = 0$. This completes the proof of (2).

When $\mathrm{char}(K) = 0$, similar inductive argument plus Gauss Lemma will work. We leave it to the readers. □

Finally, if $K = \mathbb{Q}$ then the cyclotomic extension behave even nicer.

Proposition 3.9.6. *$F = \mathbb{Q}(\zeta)$ be the n-th cyclotomic extension over $\mathbb{Q}$. Then*
1. *$g_n(x)$ is irreducible.*
2. *$[F : bQ] = \varphi(n)$.*
3. *$\mathrm{Gal}_{\mathbb{Q}} F \cong \mathbb{Z}_n^*$.*

Example 3.9.7.

Consider the 3-rd cyclotomic extension over $\mathbb{F}_7$. Then $g_3(x) = \frac{x^3-1}{x-1} = (x-2)(x-4)$ is not irreducible. □

Proof. Asuuming (1), then $F = \mathbb{Q}[\zeta]$ is generated by ζ, where minimal polynomial of ζ over $\mathbb{Q}$ is $g_n(x)$. Thus $[\mathbb{Q}[\zeta] : \mathbb{Q}] = deg(g_n(x)) = \varphi(n)$. Morover, for every $i \in \mathbb{Z}_n^*$, the map $\zeta \mapsto \zeta^i$ produces an $\mathbb{Q}$-automorphism of F. Thus (3) follows.

It thus suffices to prove (1). Recall that $g_n(x) \in \mathbb{Z}[x]$. If $g_n(x) = f(x)h(x) \in \mathbb{Z}[x]$, where $f(x)$ is an irreducible polynomial with $f(\zeta) = 0$. We claim that ζ^p is also a root of $f(x)$ for all $(p, n) = 1$. Grant this claim, then by this process, we can conclude that ζ^i is a root of $f(x)$ for all $(i, n) = 1$. Therefore, $f(x) = g_n(x)$ is irreducible.

We now prove the claim. Suppose on the contrary that ζ^p is not a root of $f(x)$. Then it's a root of $h(x)$. We have $h(\zeta^p) = 0$. Hence ζ is a root of $h(x^p)$. Since $f(x)$ is irreducible, it's minimal polynomial of ζ over $\mathbb{Q}$. We have $f(x)|h(x^p)$. Thus we can write $h(x^p) = f(x)k(x)$ for some $k(x)$ in $\mathbb{Q}[x]$. By Gauss' Lemma, this equation holds in fact in $\mathbb{Z}[x]$. We now consider ring homomorphism $\bar{\cdot}\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Then

$$(\overline{h(x)})^p = \overline{h(x^p)} = \overline{f(x)k(x)}.$$

Thus $g.c.d(\overline{h(x)}, \overline{h(x)}) \neq 1$ in $\mathbb{Z}_p[x]$. It follows that

$$\overline{x^n - 1} = (\overline{\frac{x^n - 1}{g_n(x)}})\overline{f(x)h(x)}$$

has multiple roots. But $\overline{x^n - 1}' = n\bar{x}^{n-1} \neq 0$. So this is the required contradiction. $\square$