Field Theory Qual Review

Robert Won
Prof. Rogalski

1 (Some) qual problems

• (Fall 2007, 5) Let $F$ be a field of characteristic $p$ and $f \in F[x]$ a polynomial $f(x) = \sum f_i x^i$. Give necessary and sufficient conditions on the $\{f_i\}$ for $f(x^p)$ to itself be a $p^{th}$ power, i.e. $\exists g(x)$ such that $f(x^p) = g(x)^p$. In particular, prove that your condition is necessary.

• (Fall 2007, 6) Let $F/K$ be a field extension of degree 2
  a. If $K$ is characteristic not 2, show that $F/K$ is Galois.
  b. Give an example where $F/K$ is Galois even though char $K = 2$.
  c. Give an example where $F/K$ is not Galois.

• (Fall 2009, 3) Let $F$ be a finite field of order $q$ and $E/F$ a field extension. Suppose that an element $a \in E$ is algebraic over $F$. Prove that $[F(a) : F]$ is the smallest positive integer $n$ such that $a^{q^n} = a$ and that it divides every other such positive integer.

• (Fall 2009, 4) Let $G$ be any finite group and $F$ any field. Show that there exist fields $L$ and $E$ with $F \subseteq L \subseteq E$, such that $E$ is Galois over $L$ with the Galois group of $E/L$ being isomorphic to $G$.

• (Fall 2009, 5) Consider the splitting field of $E$ of the polynomial $f(x) = x^4 - 5$ over $\mathbb{Q}$.
  a. Find the degree $[E : \mathbb{Q}]$
  b. Determine the Galois group of $E$ over $\mathbb{Q}$ as a subgroup of $S_4$.

• (Spring 2008, 4) Suppose that there exists an intermediate field $L$ of the Galois extension $F/E$ of degree 2 over $E$. What can we say about $\text{Gal}(F/E)$?

• (Spring 2009, 4) Let $a = \sqrt{2} + \sqrt{2}$ in $\mathbb{C}$ and let $f$ be the minimal polynomial of $a$ over $\mathbb{Q}$. Let $E$ be the splitting field for $f$ over $\mathbb{Q}$. Determine the Galois group $\text{Gal}(E/\mathbb{Q})$.

• (Spring 2009, 5) Let $E/F$ be a Galois extension and let $K, L$ be intermediate fields. Show that $K$ and $L$ are $F$-isomorphic (i.e. there exists an isomorphism from $K$ to $L$ which is the identity on $F$) if and only if the subgroups of $G = \text{Gal}(E/F)$ corresponding to $K$ and $L$ are conjugate in $G$. 
2 (Some) field things to know

Throughout, $F$ and $K$ are fields.

- Basic facts and definitions. (characteristic, prime subfield, field extension, degree of a field extension, field extensions generated by elements, primitive elements, algebraic extensions)
- The characteristic of $F$ is either 0 or prime.
- Any homomorphism of fields is 0 or injective.
- Let $p(x) \in F[x]$ be irreducible. Then there exists a field extension $K/F$ in which $p(x)$ has a root. In particular, $K = F[x]/p(x)$ and $[K : F] = n$. If $\deg p(x) = n$ and $\theta = x \mod (p(x)) \in K$ then $1, \theta, \ldots, \theta^{n-1}$ are an $F$-basis for $K$.
- Let $p(x) \in F[x]$ be irreducible. If $K$ is an extension of $F$ containing $\alpha$ a root of $p(x)$ then $F(\alpha) \cong F[x]/p(x)$.
- Let $\varphi : F \rightarrow F'$ be an isomorphism of fields and $p(x) \in F[x]$ be irreducible. Let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying $\varphi$ to the coefficients. Let $\alpha$ be a root of $p(x)$ and $\beta$ be a root of $p'(x)$. Then there is an isomorphism
  \[\sigma : F(\alpha) \rightarrow F'(\beta)\]
such that $\sigma(\alpha) = \beta$ and $\sigma|_F = \varphi$.
- Let $\alpha$ be algebraic over $F$. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has $\alpha$ as a root. The polynomial $m_{\alpha,F}(x)$ is called the minimal polynomial and its degree is called the degree of $\alpha$.
- If $L/F$ is an extension of fields and $\alpha$ is algebraic over $F$ and $L$ then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L$.
- Let $\alpha$ be algebraic over $F$, then $F(\alpha) \cong F[x]/(m_{\alpha}(x))$ and $[F(\alpha) : F] = \deg m_{\alpha}(x) = \deg \alpha$.
- The element $\alpha$ is algebraic over $F$ if and only if $F(\alpha)/F$ is finite.
- If $K/F$ is finite, then it is algebraic.
- If $F \subseteq K \subseteq L$ are fields then $[L : F] = [L : K][K : F]$.
- The extension $K/F$ is finite if and only if $K$ is generated by a finite number of algebraic elements over $F$.
- If $\alpha$ and $\beta$ are algebraic over $F$ then $\alpha \pm \beta$, $\alpha \beta$, $\alpha/\beta$ are all algebraic.
- Let $L/F$ be an arbitrary extension. Then the collection of elements of $L$ that are algebraic over $F$ form a subfield $K$ of $L$.
- If $K$ is algebraic over $F$ and $L$ algebraic over $K$ then $L$ is algebraic over $F$. 
Let $K_1$ and $K_2$ be two finite extensions of a field $F$ contained in $K$. Then

$$[K_1K2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an $F$-basis for one of the fields remain linearly independent over the other field.

- Splitting fields exist and the splitting field of a polynomial is unique up to isomorphism.
- If $K$ is an algebraic extension of $F$ which is the splitting field over $F$ for some collection of polynomials, then $K$ is called a normal extension of $F$.
- A splitting field of a polynomial of degree $n$ has degree at most $n!$.
- A polynomial $f(x)$ has a multiple root $\alpha$ if and only if $\alpha$ is also a root of its derivative. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative.
- Every irreducible polynomial over a field of characteristic 0 or a finite field is separable.
- If $\text{char } F = p$ then $(a + b)^p = a^p + b^p$ and $(ab)^p = a^pb^p$.
- Let $p(x)$ be an irreducible polynomial over $F$ a field of characteristic $p$. Then there exists a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{\text{sep}}(x) \in F[x]$ such that

$$p(x) = p_{\text{sep}}(x^p).$$

- Every finite extension of a perfect field is separable.

**Cyclotomic polynomials:** Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity. The $n^{\text{th}}$ cyclotomic polynomial $\Phi_n(x)$ is the degree $\varphi(n)$ polynomial whose roots are the primitive $n^{\text{th}}$ roots of unity:

$$\Phi_n(x) = \prod_{\zeta \text{ primitive}} (x - \zeta) = \prod_{(a,n)=1} (x - \zeta_n^a).$$

$\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ which is the unique irreducible monic polynomial of degree $\varphi(n)$.

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

- Let $K/F$ be a field extension and $\alpha \in K$ algebraic over $F$. Then for any $\sigma \in \text{Aut}(K/F)$, $\sigma \alpha$ is a root of the minimal polynomial for $\alpha$ over $F$; that is $\text{Aut}(K/F)$ permutes the roots of irreducible polynomials.
- $|\text{Aut}(E/F)| \leq [E : F]$
• **Galois extensions**: $K/F$ is Galois if any of the following equivalent conditions hold

1. $K/F$ is a splitting field of a collection of separable polynomials over $F$
2. $F$ is the precisely the set of elements fixed by $\text{Aut}(K/F)$ (in general, the fixed field may be larger than $F$)
3. $[K : F] = |\text{Aut}(K/F)|$
4. $K/F$ is finite, normal, and separable

• (Fundamental Theorem of Galois Theory) Let $K/F$ be a Galois extension and $G = \text{Gal}(K/F)$. Then there is a bijection

$$\{\text{subfields } E \text{ of } K \text{ containing } F\} \leftrightarrow \{\text{subgroups } H \text{ of } G\}$$

given by the correspondence

$$E \rightarrow \{\text{the elements of } G \text{ fixing } E\}$$

$$\{\text{the fixed field of } H\} \leftarrow H$$

which are inverse. Under this correspondence,

1. $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$
3. $K/E$ is Galois with Galois group $H$
4. $E/F$ is Galois if and only if $H$ is normal. In this case, the Galois group of $E/F$ is $G/H$.
5. The intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ and the composite field $E_1E_2$ corresponds to $H_1 \cap H_2$.

• Any finite field is isomorphic to $\mathbb{F}_{p^n}$ which is the splitting field over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$, with cyclic Galois group of order $n$ generated by the Frobenius automorphism $\sigma_p$. The subfields of $\mathbb{F}_{p^n}$ are the fields $\mathbb{F}_{p^d}$ and are all Galois over $\mathbb{F}_p$, they are the fixed fields of $\sigma_p^d$ for $d \mid n$.

• The finite field $\mathbb{F}_{p^n}$ is simple.

• The polynomial $x^{p^n} - x$ is the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree $d$ where $d$ runs across the divisors of $n$.

• The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of $n^{th}$ roots of unity is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is given by

$$(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

$$a \mod n \mapsto \sigma_a$$

where $\sigma_a(\zeta_n) = \zeta_n^a$.

• The extension $K/F$ is called abelian if $K/F$ is Galois and $\text{Gal}(K/F)$ is abelian.

• If $G$ is any finite abelian group, then there is a subfield $K$ of the a cyclotomic field with $\text{Gal}(K/\mathbb{Q}) \cong G$. 

4