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 $f(x) = \sum_i f_i x^i$. 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.

  Each i should be a multiple of p and each f_i should be a pth power. Then use the Frobenius endomorphism.

- (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.

     Take any $\alpha \in F \setminus K$. Then the minimal polynomial of α over K will be degree 2. Further, $F \cong K(\alpha)$. Now the minimal polynomial of α will be separable as long as the characteristic is not 2 so F will be the splitting field of a separable polynomial over K and hence Galois.

  b. Give an example where F/K is Galois even though $\operatorname{char} K = 2$.

     Any degree 2 irreducible polynomial which is separable will give you such an extension. Take the splitting field of $x^2 + 1$, over $\mathbb{F}_2$, for example.

  c. Give an example where F/K is not Galois.

     You can adjoin a root of a degree 2 irreducible which is not separable (in fact this is the only thing that will work). This is not possible over a finite field. Your first attempt should always be with $\mathbb{F}_2(t)$ as your field and indeed, $x^2 - t$ is an irreducible (by Eiseinstein, say) which is not separable (by the gcd condition on the derivative). Hence, adjoining a root it gives a degree 2 field extension which is not Galois (you can see this since it will only contain one root of $x^2 - t$).

- (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.

  You should use the characterization of finite fields as $\mathbb{F}_{p^n}$ for some prime p and some natural number n. Each $\mathbb{F}_{p^n}$ can be realized as the splitting field of $x^{p^n} - x$.

- (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.

Let $|G| = n$ and let $s_1, \ldots, s_n$ be the elementary symmetric polynomials in indeterminates $x_1, \ldots, x_n$. You should use the theorem that $F(x_1, \ldots, x_n)$ is Galois over $F(s_1, \ldots, s_n)$ with Galois group S_n. G is a subgroup of S_n and now use the FTGT.

- (Fall 2009, 5) Consider the splitting field of E of the polynomial $f(x) = x^4 - 5$ over $\mathbb{Q}$.

  a. Find the degree $[E : \mathbb{Q}]$

  You can adjoin a fourth root of unity ζ_4 and $\sqrt[4]{5}$ to $\mathbb{Q}$. Show that this is exactly the splitting field. The minimal polynomials are the cyclotomic polynomial Φ_4 (which has degree 2, use the formula for degrees of cyclotomics) and $x^4 - 5$ (which has degree 4, duh). The cyclotomic is still irreducible after adjoining $\sqrt[4]{5}$, so teh extension should have degree 8.

  b. Determine the Galois group of E over $\mathbb{Q}$ as a subgroup of S_4.

  The roots of $x^4 - 5$ are $\zeta_4^i \sqrt[4]{5}$ where $1 \leq i \leq 4$. Use i to label the roots. Since the extension is Galois you can send any root to any other root. Track where the other roots go to find the Galois group as an explicit 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 $\mathrm{Gal}(F/E)$?

  Straight FTGT, playa. There is a subgroup of index 2 in the Galois group. Which is normal. So $\mathrm{Gal}(F/E)$ can't be simple.

- (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 $\mathrm{Gal}(E/\mathbb{Q})$.

  Observe that $a^2 = 2 + \sqrt{2}$ and $a^4 = 6 + 4\sqrt{2}$ so a satisfies the polynomial $x^4 - 4x^2 + 2$. This is irreducible by Eisenstein, so is the minimal polynomial f. Now find all four roots (which should be $\pm\sqrt{2 \pm \sqrt{2}}$ and proceed as above to find the Galois group as a subgroup of S_4.

- (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 $G = \mathrm{Gal}(E/F)$ corresponding to K and L are conjugate in G.

  Don't panic and do each direction separately. If there is an isomorphism $\theta : K \to L$ which fixes F, then you can lift θ to an isomorphism $\tilde{\theta} : E \to E$ which restricts to θ. Then show that conjugation by $\tilde{\theta}$ gives the desired result.

  Conversely, if they are conjugate, then there exists a $\psi \in \mathrm{Gal}(E/F)$ such that $\psi \,\mathrm{Gal}(E/K)\psi^{-1} = \mathrm{Gal}(E/L)$. Show that ψ restricted to K gives the desired isomorphism.

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 α a root of $p(x)$ then $F(\alpha) \cong F[x]/p(x)$.
- Let $\varphi : F \to F'$ 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 φ to the coefficients. Let α be a root of $p(x)$ and β be a root of $p'(x)$. Then there is an isomorphism

  $$\sigma : F(\alpha) \to F'(\beta)$$

  such that $\sigma(\alpha) = \beta$ and $\sigma|_F = \varphi$.
- Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. The polynomial $m_{\alpha,F}(x)$ is called the minimal polynomial and its degree is called the degree of α.
- If L/F is an extension of fields and α is algebraic over F and L then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in L.
- Let α 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 α 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 α and β are algebraic over F then $\alpha \pm \beta$, $\alpha\beta$, α/β 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 α if and only if α 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 $\operatorname{char} F = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.
- 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

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

- Every finite extension of a perfect field is separable.
- **Cyclotomic polynomials**: Let ζ_n be a primitive n^{th} root of unity.

  The n^{th} cyclotomic polynomial $\Phi_n(x)$ is the degree $\varphi(n)$ polynomial whose roots are the primitive n^{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 $\varphi(n)$.

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

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

- Let K/F be a field extension and $\alpha \in K$ algebraic over F. Then for any $\sigma \in \operatorname{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F; that is $\operatorname{Aut}(K/F)$ permutes the roots of irreducible polynomials
- $|\operatorname{Aut}(E/F)| \leq [E : F]$
- **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 $\operatorname{Aut}(K/F)$ (in general, the fixed field may be larger than F
  (3) $[K : F] = |\operatorname{Aut}(K/F)|$
  (4) K/F is finite, normal, and separable

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

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

given by the correspondence

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

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

which are inverse. Under this correspondence,

(1) $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$

(2) $[K : E] = |H|$ and $[E : F] = |G : H|$

(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 σ_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 σ_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

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \pmod n &\mapsto \sigma_a \end{aligned}$$

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

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

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