Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2018

Midterm Exam 2 Review Sheet

Directions: The second midterm exam will take place in class on Tuesday, April 10. You will have the entire class period, 75 minutes, to complete the exam. No electronic devices will be allowed. No notes will be allowed. On all problems, you will need to write your thoughts/proofs in a coherent way to get full credit.

Topics covered and practice problems:

- Field automorphisms. The group $\mathrm{Aut}_F K$ for a field extension K/F. The bound $|\mathrm{Aut}_F K| \leq [K : F]$ for a finite extension K/F. Examples of towers $K/E/F$ where an F-automorphism of E does not lift to an F-automorphism of K.
- Galois extensions. A finite extension K/F is Galois iff $|\mathrm{Aut}_F K| = [K : F]$, in which case we call $\mathrm{Gal}(K/F) := \mathrm{Aut}_F K$ the Galois group of K/F. Also, a finite extension is Galois iff it is normal and separable. Galois correspondence: given a Galois extension K/F with group G, there is an inclusion reversing bijection between the lattices

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Subextensions} \\ K/E/F \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{Subgroups} \\ H \leqslant G \end{array} \right\} \\ E & \longmapsto & \mathrm{Gal}(K/E) \\ K^H & \longmapsfrom & H \end{array}$$

  with the properties that $[E : F] = [G : H]$ and that E/F is Galois iff $H \trianglelefteqslant G$, in which case $\mathrm{Gal}(E/F) \cong G/H$.
- Galois perspective on quadratic and cubic extensions. Discriminant.

  If F has characteristic $\neq 2$ and K/F is quadratic, then $K = F(\sqrt{a})$ for some $a \in F$ and K/F is Galois with group C_2 generated by $\sqrt{a} \mapsto -\sqrt{a}$. Know examples of quadratic Galois extensions over some characteristic 2 fields, e.g. $\mathbb{F}_2$ and $\mathbb{F}_2(t)$.

  If F has characteristic $\neq 2$ and K/F is a separable cubic extension with $K = F(\alpha)$, where α has minimal polynomial $f(x) \in F[x]$, then K/F is Galois with group C_3 iff the discriminant $\Delta(f)$ is a square in F. If $\Delta(f)$ is not a square, then $\mathrm{Aut}_F K$ is trivial and K/F is not normal (in particular, not Galois), in which case the normal closure of K/F is $K(\sqrt{\Delta(f)})$ and it is Galois over F with group S_3. Know examples of cubic Galois extensions over some characteristic 2 fields, like $\mathbb{F}_2$ and $\mathbb{F}_2(t)$.

  In general, if K/F is the splitting field of a polynomial $f(x) \in F[x]$ of degree n, then $\mathrm{Aut}_F K \leqslant S_n$. The discriminant $\Delta(f) \in F$ is nonzero iff K/F is separable, in which case K/F is Galois. If also the characteristic of F is not 2, then $\Delta(f)$ is a square in F iff $\mathrm{Gal}(K/F) \leqslant A_n$.
- Normality. A finite extension K/F is normal iff it is the splitting field of a polynomial. Transitivity properties (or failure thereof, with examples to keep in mind) of normality in a tower $K/E/F$. Think of an inseparable normal extension. If a finite extension K/F is not normal, then it has a normal closure $N/K/F$, of minimal degree over K such that N/F is normal, and which is unique up to F-isomorphism. For example, the normal closure of a simple extension $F(\alpha)/F$ is the splitting field of the minimal polynomial of α.

- Separability of polynomials. A polynomial $f(x) \in F[x]$ is separable iff it has simple roots in its splitting field iff it has simple roots in any field where it splits completely iff $f(x)$ and $f'(x)$ are relatively prime. An irreducible polynomial $f(x) \in F[x]$ is separable iff $f'(x)$ is nonzero. If F has characteristic zero, then any irreducible polynomial is separable. If F has characteristic $p > 0$, then any irreducible polynomial $f(x) \in F[x]$ has the form $f(x) = g(x^{p^n})$ where $g(x) \in F[x]$ is irreducible and separable and $n \geq 0$; in this case, $f(x)$ is inseparable iff $n > 0$.

  Separability of elements and extensions K/F. An element $\alpha \in K$ is separable over F if its minimal polynomial over F is separable. An extension K/F is separable iff every element is separable over F iff it is generated by elements separable over F. Transitivity properties of separability. Purely inseparable extensions. Factoring any algebraic extension into a separable extension followed by a purely inseparable extension. Examples of (purely) inseparable extensions.

- Derivations $\mathrm{Der}(R)$ on a commutative unital ring R and F-derivations $\mathrm{Der}_F(R)$ on a commutative unital F-algebra R. Derivations and F-derivations on the polynomial ring $F[x]$ and the rational function field $F(x)$. A finite extension K/F is separable iff every derivation of F extends uniquely to a derivation on K iff $\mathrm{Der}_F K = 0$. Formula for the extension of a derivation to a separable extension and examples of nonuniqueness of extensions to an inseparable extension (e.g., nonzero F-derivations on an inseparable extension K/F).

- Finite fields. Classification in terms of number of elements $q = p^n$. Frobenius automorphism and Galois groups of extensions of finite fields. Construction as the splitting field of $x^q - x$.

- Embeddings. For extensions E/F and K/F, the set of F-embeddings $\mathrm{Hom}_F(E, K)$ versus the K-vector space of F-linear maps $\mathrm{Hom}_{F\text{-vs}}(E, K)$. The extension theorem: the set of F-embeddings of a simple extension $F(\alpha) \to K$ are in bijection with the set of roots of the minimal polynomial of α over F that are contained in K. The automorphism group $\mathrm{Aut}_F K$ acts transitively on the roots of any irreducible polynomial over F that splits completely over K. Linear independence of characters and embeddings (Dedekind Lemma). If E/F is finite and N/F normal, then $|\mathrm{Hom}_F(E, N)| \leq [E : F]$ with equality iff E/F is separable.

Explicit examples to study:

- The lattice of subfields (and corresponding subgroups) of the Galois extension $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ with group S_3, which is the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

- The lattice of subfields (and corresponding subgroups) of the Galois extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ with group C_4. What nice polynomial is this the splitting field of?

- The lattice of subfields (and corresponding subgroups) of the Galois extension $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ with group D_8, which is the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

- The lattice of subfields (and corresponding subgroups) of the Galois extension of finite fields $\mathbb{F}_{256}/\mathbb{F}_2$.

- The extension $\mathbb{F}_p(t)[x]/(x^n - t)$ over $\mathbb{F}_p(t)$ for various values of n. (By the way, it's easy to see that $x^n - t$ is irreducible over $\mathbb{F}_p(t)$ using the Eisenstein criterion over $\mathbb{F}_p[x]$, and you should know how this works.) You already know that for $n = p$, this extension is purely inseparable. What about when n is relatively prime to p? Generally, in terms of n, how does this extension factor as a separable extension and then a purely inseparable extension?