Math 206C: Algebra
Midterm 2 (Galois Theory): Things to Know

In this document, we give some definitions, examples, and theorems that will be helpful to know for Midterm 2. This document will focus on our unit on Galois theory: Lectures 16-20.

Galois Theory

Definitions

1. Automorphisms of a field. The groups $\mathrm{Aut}(K)$ and $\mathrm{Aut}(K/F)$.
2. The fixed field of $H \leq \mathrm{Aut}(K)$, K^H.
3. What it means for a finite extension K/F to be a Galois extension.
   The Galois group of K/F.
4. The Galois conjugates of an element.
5. An embedding of a field K into a field L.

Examples

1. $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$.
2. $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. (Not a Galois extension– 'not enough roots' of $x^3 - 2$.)
3. $\mathrm{Aut}(\mathbb{F}_p(u^{1/n})/\mathbb{F}_p(u))$. (Not a Galois extension– not separable.)
4. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a Galois extension. Galois group is isomorphic to S_3.
   Fixed field for each subgroup. (Example (4) pages 563-564 in Section 14.1)
5. $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ is a Galois extension. Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   Fixed field for each subgroup. (Example (5) page 564 in Section 14.1)
6. $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ is a Galois extension. Galois group is isomorphic to D_4. Fixed field for each subgroup. (Example 4.7 and 5.9 in Conrad's 'The Galois Correspondence' notes.)
7. Let K be a quadratic extension of F, where F is a field of characteristic not equal to 2.
   Then K/F is Galois. (Example (2) page 563 in Section 14.1)
8. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.
   (Example (7) page 566 in Section 14.1)

Theorems

1. If $F_1 \subseteq F_2 \subseteq K$ then $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$. If $H_1, H_2 \leq \mathrm{Aut}(K)$ then $K^{H_2} \subseteq K^{H_1}$. (Proposition 4 in Section 14.1.)
2. $F \subseteq K^{\mathrm{Aut}(K/F)}$ and $H \subseteq \mathrm{Aut}(K/K^H)$.
3. If $\sigma \in \mathrm{Aut}(K/F)$ and $f(x) \in F[x]$ then $\sigma(f(\alpha)) = \sigma(f(\alpha))$ for all $\alpha \in K$.
   In particular, $\sigma \in \mathrm{Aut}(K/F)$ permutes the roots of $f(x)$ in K.
4. If K/F is finite, then $\mathrm{Aut}(K/F)$ is finite.
5. Let $f(x) \in F[x]$ and E be a splitting field of $f(x)$ over F. Then $|\mathrm{Aut}(E/F)| \leq [E\colon F]$ where equality holds if $f(x)$ is separable over F. If K is a splitting field for a separable polynomial $f(x)$ over F, then K/F is Galois. (Proposition 5 and Corollary 6 in Section 14.1.)
6. Let G be a subgroup of $\mathrm{Aut}(K)$ and let F be the fixed field of G. Then $[K\colon F] = |G|$. (Theorem 9 in Section 14.2. You should know the statement of this result, but we have not yet talked about the proof.)
7. Let K/F be a finite extension. Then $|\mathrm{Aut}(K/F)| \mid [K\colon F]$.
   $|\mathrm{Aut}(K/F)| = [K\colon F]$ if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. (Cor 10 Section 14.2)
8. Let G be a finite subgroup of $\mathrm{Aut}(K)$ and let F be the fixed field of G. Then $\mathrm{Aut}(K/F) = G$. (Corollary 11 in Section 14.2)
9. If $G_1 \neq G_2$ are distinct finite subgroups of $\mathrm{Aut}(K)$ then $K^{G_1} \neq K^{G_2}$.
   (Corollary 12 in Section 14.2)
10. If K/F is Galois then every irreducible polynomial in $F[x]$ that has a root in K is separable and has all of its roots in K.
    (We called this Proposition 13* in lecture– it is part of Theorem 13 in Section 14.2.)
11. If K/F is Galois and $\alpha \in K$, the roots of $m_{\alpha,F}(x)$ are the distinct Galois conjugates of α over F.
12. K/F is Galois if and only if K is the splitting field of some separable polynomial over F. (Theorem 13 in Section 14.2)
13. Let K/F be a finite extension. The following are equivalent:
    (a) $[K\colon F] = |\mathrm{Aut}(K/F)|$.
    (b) K is the splitting field over F of a separable polynomial $f(x) \in F[x]$.
    (c) $K^{\mathrm{Aut}(K/F)} = F$.
    (d) K is separable and every irreducible polynomial $F[x]$ that has a root in K has all of its roots in K.
14. The Fundamental Theorem of Galois Theory
    (Theorem 14 in Section 14.2. In Lecture 20 we stated and proved all parts of this theorem except part (5), which we proved in Lecture 21.)