Math 206C: Algebra
Final Exam: Things to Know

In this document, we give some definitions, examples, and theorems that will be helpful to know for the Final Exam. This document will focus on the material we covered in the course that was not covered on Midterm 2 (Lectures 21-28).

Definitions

1. The Galois closure of E over F.
2. Simple Extensions and Primitive Elements.
3. Abelian extension. Cyclic extension.
4. The Galois group of a separable polynomial $f(x) \in F[x]$.
5. Elementary symmetric functions. The general polynomial of degree n over F.
6. The discriminant of $x_1, \ldots, x_n$. The discriminant of a polynomial.
7. The resolvent cubic of a quartic $g(y) = y^4 + py^2 + qy + r$.
   (I do not expect you to be able to write out the coefficients of this polynomial, but you should be able to define it in terms of the roots of $g(y)$.)

Examples

1. Examples of the Galois Correspondence: $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ (computing the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$), $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$.
2. The number of irreducible polynomials of degree 4 in $\mathbb{F}_p[x]$.
3. An example showing that the assumption that at least one of K, F' is Galois over F really is necessary to apply Corollary 20 in Section 14.4.
4. Examples of Galois closures.
5. The Galois correspondence for cyclotomic fields: The quadratic subfield $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ of $\mathbb{Q}(\zeta_5)$. The cubic subfield of $\mathbb{Q}(\zeta_7)$ (and the minimal polynomial of a primitive element for it).
6. Galois groups as subgroups of permutation groups. Examples: $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
7. The discriminant of a quadratic polynomial $x^2 + ax + b$.
   The discriminant of a cubic polynomial $y^3 + py + q$.
8. Computing the Galois group of a cubic polynomial $f(x) \in F[x]$ where $\mathrm{char}(F) \neq 2, 3$.

9. Computing the Galois group of a quartic polynomial $f(x) \in F[x]$ where $\text{char}(F) \neq 2, 3$.
(I do not expect you to know all of the details here, but you should understand the major pieces that go into this procedure.)

Theorems

1. 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.)

2. The Galois correspondence for finite extensions of $\mathbb{F}_p$. Proposition 15 in Section 14.3.
You should be aware of how this result generalizes to finite extensions of a general finite field $\mathbb{F}_q$. Exercise 9 of Section 14.3.

3. $\mathbb{F}_{p^n}$ is a simple extension of $\mathbb{F}_p$. There exists an irreducible polynomial of degree n over $\mathbb{F}_p$ for each $n \geq 1$.

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

5. Let $\mathbb{F}_q$ be a finite field of order $q = p^m$. Suppose $p \nmid n$. Let K be the splitting field of $x^n - 1$ over $\mathbb{F}_q$. Then $[K : \mathbb{F}_q]$ is the smallest positive integer d such that $n \mid (q^d - 1)$.
(That is, d is the order of q in $(\mathbb{Z}/n\mathbb{Z})^*$.)

6. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension with $\text{Gal}(KF'/F') \cong \text{Gal}(K/(K \cap F'))$, which is isomorphic to a subgroup of $\text{Gal}(K/F)$. (Proposition 19 in Section 14.4.)
Its consequence for degrees of composite extensions (Corollary 20) is often useful.

7. Intersections and composites of Galois extensions are Galois. Description of $\text{Gal}(K_1K_2/F)$ in terms of $\text{Gal}(K_1/F)$ and $\text{Gal}(K_2/F)$. (Proposition 21 in Section 14.4.)

8. Let E/F be a finite separable extension. Then E is contained in an extension K that is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extensions of F containing E contains K. (Corollary 23 in Section 14.4.)

9. The Primitive Element Theorem.

10. $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. (Theorem 26 in Section 14.5)

11. The primitive n^{th} roots of unity give a basis of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ iff n is squarefree.
(Exercise 11 in Sectioin 14.5)

12. Composites and intersections of cyclotomic fields.

13. Generators for subfields of $\mathbb{Q}(\zeta_p)$– the elements α_H.

14. Suppose E is the splitting field of a separable polynomial $f(x) \in F[x]$ of degree n. Then $\text{Gal}(E/F)$ is isomorphic to a subgroup of S_n. If $f(x)$ is irreducible, then this subgroup is transitive.

15. The general polynomial $x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n$ is separable with Galois group S_n. (Theorem 32 in Section 14.6– I would not ask you to prove this on an exam.)

16. Suppose F is a field of characteristic not equal to 2. Let $f(x) \in F[x]$ be separable of degree n. Fix an ordering of the roots of $f(x)$ and view $\mathrm{Gal}(f)$ as a subgroup of S_n. Then $\mathrm{Gal}(f)$ is a subgroup of A_n if and only if the discriminant of F is the square of an element in F.

17. An irreducible cubic $f(x) \in \mathbb{Q}[x]$ with exactly one real root has $\mathrm{Gal}(f) \cong S_3$. Its generalization: Let p be prime. An irreducible $f(x) \in \mathbb{Q}[x]$ with degree p and exactly $p-2$ real roots has Galois group S_p.

18. Let $K/\mathbb{Q}$ be a finite Galois extension (where $K \subset \mathbb{C}$). Then complex conjugation restricts to an element of $\mathrm{Gal}(K/\mathbb{Q})$. This element is trivial if $K \subset \mathbb{R}$ and has order 2 otherwise.

19. The Fundamental Theorem of Algebra.
(You do not need to know the proof, but you should definitely know the statement.)