Mike O'Sullivan
Department of Mathematics
San Diego State University Fall 2012

Math 627A: Modern Algebra I
Homework VII

Due Th. 12/13 2012 (if you need more time for Problem 3, ask).

Problem 1: In a group G, the *commutator* of a, b is $aba^{-1}b^{-1}$. Notice that this is e_G iff a and b commute. The *commutator subgroup* of a group G is the group G' generated by the commutators.

$$G' = \langle aba^{-}b^{-1} : a, b \in G \rangle$$

(a) Compute the commutator subgroup of D_n (two cases: n odd and n even).

(b) Compute the commutator of the conjugation of a by x and the conjugation of b by x.

(c) Prove that G' is a normal subgroup of G. It is enough to show that the conjugation of any commutator is another commutator.

(d) Prove that G/G' is abelian.

(e) Prove that G/N abelian implies $G' \leq N$.

Problem 2: Let H_1 and H_2 be two subgroups of G, the *join* of H_1 and H_2 is the smallest subgroup of G containing H_1 and H_2. It is the intersection of all groups containing $H_1 \cup H_2$, which we have written as $\langle H_1 \cup H_2 \rangle$. In Galois theory it is often written $H_1 \vee H_2$. Let E_1 and E_2 be two subfields of K. Their *join* (also called the compositum) $E_1 \vee E_2$ is the smallest subfield containing both E_1 and E_2. Let K be a Galois extension of F. Let E_1 and E_2 be two intermediate fields and let H_1, H_2 be subgroups of $G = \mathrm{Gal}(K/F)$.

(a) Explain why $\mathcal{G}(E_1 \vee E_2) = \mathcal{G}(E_1) \cap \mathcal{G}(E_2)$. [One direction is easy, the other just requires an understanding of the elements of $E_1 \vee E_2$.]

(b) Explain why $\mathcal{F}(H_1 \vee H_2) = \mathcal{F}(H_1) \cap \mathcal{F}(H_2)$. [Again, one direction is easy, the other just requires an understanding of the elements of $H_1 \vee H_2$.]

(c) Now use Galois' main theorem to show that $\mathcal{F}(H_1 \cap H_2) = \mathcal{F}(H_1) \vee \mathcal{F}(H_2)$ and $\mathcal{G}(E_1 \cap E_2) = \mathcal{G}(E_1) \vee \mathcal{G}(E_2)$.

Problem 3: Let E be the splitting field of $x^6 - 2$.

(a) Show that $x^6 - 2$ is irreducible over $\mathbb{Q}$.

(b) Explain why the Galois group is isomorphic to D_6, the dihedral group on 6 elements.

(c) Find the Galois group and map out the relationship between subfields and subgroups for $E/\mathbb{Q}$.

Math 627A: Modern Algebra I
Final Test

For the final exam you will write about the 4 topics listed below. Imagine you are writing for fellow master's students. Your goal is to explain to them the essential aspects of the topic, but also to make it interesting.

Grading will be based on

(1) Grammar: Are you using symbols correctly?

(2) Essential correctness: Are definitions, statements of theorems, and other fundamental concepts correctly and completely stated?

(3) Elaboration: Do you have interesting examples, proofs of theorems or insightful discussion that bring the subject to life?

Plan on roughly 20 minutes for topics A, C, D and 30 minutes for B, plus an additional 30 minutes to polish and finalize.

Topic A: Explain separability and normality for field extensions. Define the terms, but also enrich the discussion.
Grammar 20 pts. Essential correctness 20 pts. Elaboration 30 pts.

Topic B: Explain the Fundamental Theorem of Galois Theory concerning field extensions and automorphism groups. State the theorem including discussion of containment, intersections, and normality, enrich with a proof or examples.
Grammar 30 pts. Essential correctness 30 pts. Elaboration 50 pts.

Topic C: Discuss the Galois correspondence for a small cyclotomic field extension (that will be given on the day of the exam).
Grammar 20 pts. Correctness 30 pts.

Topic D: Discuss the Galois correspondence for finite fields. For $\mathbb{F}_{p^n}$, describe the Galois group, identify all the subfields and the corresponding automorphism groups. As a challenge item: Explore the relationship between the combinatorics for irreducible polynomials over $\mathbb{F}_p$ and finite fields as suggested in problem #6 on the previous test and problem 6 below.
Grammar, 20 pts. Essential correctness 20 pts. Elaboration 40 pts.

Final Grade

The final grade for the course will be out of 1100 pts. HW is 550 (including the last two assignments worth 100 each). Test is 250. Final is 300.

- Above 900 guarantee an A-
- 775 guarantees a B-
- 650 guarantees a C

Problems 1-2 give some additional practice for small field extensions.
Problems 3-4 deal with cyclotomic extensions and polynomials.
Problem 5 gives two examples of infinite extensions.
Problem 6 concerns finite fields and irreducible polynomials.

Problem 1: Minimal polynomials for elements of $\mathbb{Q}(\sqrt[3]{2})$ (see [A] 3.1#4,5).

(a) Find the minimum polynomial of $\sqrt[3]{2}+1$ over $\mathbb{Q}$. [There is a clever way that involves little computation, but don't feel obliged to use it!]

(b) Find the minimum polynomial of $\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbb{Q}$.

Problem 2: Let $E=\mathbb{Q}(i+\sqrt{2})$.

(a) Show that i and $\sqrt{2}$ are both in E.

(b) Find the minimum polynomial of $i+\sqrt{2}$.

(c) Show this polynomial splits in E.

(d) Find the Galois group and map out the relationship between subfields and subgroups for $E/\mathbb{Q}$.

Problem 3: Sixth roots of unity.

(a) Factor x^6-1 completely over $\mathbb{Q}$.

(b) Show that the splitting field of x^6-1 is of degree 2 over $\mathbb{Q}$.

Problem 4: Map out the Galois correspondence for $\mathbb{Q}(\zeta_n)$ for $n=7,9,10,11$.

Problem 5: Infinite algebraic extensions.

(a) Find a sequence of fields $\mathbb{Q}\le F_1\le F_2\le\cdots$ such that each F_i is a normal extension of $\mathbb{Q}$. Justify your answer. [See 6.3#5 for inspiration.]

(b) Find a sequence of fields $\mathbb{Q}\le F_1\le F_2\le\cdots$ such that each F_{i+1} is a normal extension of F_i but not of F_{i-1}. [See 6.3#9 for inspiration.]

Problem 6: Irreducible polynomials over $\mathbb{F}_p$. Suppose you have formulas for the number of irreducible monic polynomials of degree m over $\mathbb{F}_p$ for each $m<n$. Using some combinatorial arguments you can then compute the number of monic reducible polynomials of degree n. Subtracting this from the number of monic polynomials of degree n yields the number of monic irreducible polynomials of degree n.

(a) Show that the number of monic irreducible quadratics over $\mathbb{F}_p$ is $(p^2-p)/2$.

(b) Show that the number of monic irreducible cubics over $\mathbb{F}_p$ is $(p^3-p)/3$.

(c) You might want to guess at a general formula. A different counting method yields the result more easily than the one above. Try this if you want, noting:

- For $a\in\mathbb{F}_{p^n}$, a is in no proper subfield iff the minimal polynomial for a has degree n.
- Each monic irreducible of degree n has n distinct roots in $\mathbb{F}_{p^n}$.