Math 314 — Homework Assignment 4 — MARCH 15, 2004

DUE DATE: MARCH 23, 2004

1. Suppose that $K \subseteq L$ is a finite Galois extension, and M_1 and M_2 any two intermediate fields (i.e., $K \subseteq M_i \subseteq L$ for $i = 1, 2$). Let M be the smallest field in L containing both M_1 and M_2, and let $M' = M_1 \cap M_2$. (Another way to say this is that M' is the largest subfield of L contained in both M_1 and M_2).

If H_1 and H_2 are the subgroups of $G = \mathrm{Aut}(L/K)$ corresponding to M_1 and M_2 under the Galois correspondence, show that:

(a) The subgroup corresponding to M is $H = H_1 \cap H_2$, and

(b) the subgroup corresponding to M' is the subgroup H' generated by H_1 and H_2.

2. Recall that a group G is a product $G = H_1 \times H_2$ if and only if there are *normal* subgroups $H_1 \subset G$ and $H_2 \subset G$ such that $H_1 \cap H_2 = \{e\}$ and $H_1 \cdot H_2$ (the subgroup generated by H_1 and H_2) is equal to G.

Suppose that $K \subseteq L$ is a finite Galois extension, and M_1 and M_2 are two intermediate fields such that:

(i) Both $K \subseteq M_1$ and $K \subset M_2$ are Galois extensions.

(ii) $M_1 \cap M_2 = K$.

(iii) The smallest subfield of L containing both M_1 and M_2 is L itself.

If H_1 and H_2 are the subgroups of $G = \mathrm{Aut}(L/K)$ corresponding to M_1 and M_2 under the Galois correspondence, show that $G = H_1 \times H_2$.

Conversely, if the Galois group G is a product $G = H_1 \times H_2$, then show that there are two intermediate fields M_1 and M_2 having the properties above.

3. If $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha, \omega, \sqrt{3})$ with $\alpha = 2^{1/3}$ and $\omega = e^{2\pi i/3}$ then explain why $K \subset L$ is a Galois extension and compute $\mathrm{Aut}(L/K)$.

You may use results (without having to reprove them) from previous homework problems in answering this question. Just be sure to mention explicitly which facts you're using, and where you got them from.

4. Which of these two polynomials are irreducible over $\mathbb{F}_5$?:

(a) $x^2 + x + 2$

(b) $x^2 + x + 3$

Which of these two polynomials are irreducible over $\mathbb{F}_7$?:

(c) $x^2 + 5x - 2$

(d) $x^2 + 5x - 3$

5. For a quadratic polynomial $f(x) = ax^2 + bx + c$, the number $b^2 - 4ac$ is called the *discriminant* of $f(x)$.

(a) Compute the discriminants of the quadratic polynomials in question 4.

Note that two of the answers are numbers in $\mathbb{F}_5$ and two are numbers in $\mathbb{F}_7$.

A number $y \in \mathbb{F}_p$ is called a *square* if there is an $x \in \mathbb{F}_p$ with $x^2 = y$.

(b) List the squares in $\mathbb{F}_5$ and $\mathbb{F}_7$.

(c) Which of the discriminants are squares?

(d) What is the connection betwen the answer in (c) and the answers in question 4?

6. Suppose that L is a field with $244,140,625$ elements.

(a) What is $\mathrm{char}(L)$?

(b) If $p = \mathrm{char}(L)$, what is the index $[L : \mathbb{F}_p]$?

(c) What is the Galois group $\mathrm{Aut}(L/\mathbb{F}_p)$?

(d) Draw the diagram of subfields of L and their inclusions.