Math 306, Spring 2008
Final Exam Review Solutions

(1) Let α denote the positive fourth root of 2. Find the Galois group of x^4+2 over each of the fields: (i) $\mathbb{Q}(\sqrt{2})$, (ii) $\mathbb{Q}(\sqrt{2},i)$, (iii) $\mathbb{Q}(\alpha)$, (iv) $\mathbb{Q}(\alpha,i)$.

Solution: The splitting field of x^4+2 is $\mathbb{Q}(\alpha,i)$.
(a) The extension is given by $\mathbb{Q}(\sqrt[4]{2},i)\colon\mathbb{Q}(\sqrt{2})$, which has order 4. Notice that the automorphisms of the Galois group are determined by $\sqrt[4]{2}\mapsto\pm\sqrt[4]{2}$ and $i\mapsto\pm i$. Therefore the Galois group is $\mathbb{Z}_2\times\mathbb{Z}_2$.
(b) The extension has degree 2, so the Galois group is $\mathbb{Z}_2$.
(c) The extension has degree 2, so the Galois group is $\mathbb{Z}_2$.
(d) The extension is trivial, so the Galois group is $\langle e\rangle$.

(2) Find an extension L of $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to (a) $\mathbb{Z}_4$, (b) $\mathbb{Z}_6$, (c) $S_3\times\mathbb{Z}_{10}$.

Solution:
(a) $L=\mathbb{Q}(e^{2\pi i/5})$
(b) $L=\mathbb{Q}(e^{2\pi i/7})$
(c) $L=\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3},e^{2\pi i/11})$

(3) (a) Give an example of a field K and two nonisomorphic extensions L_1 and L_2 such that $\mathrm{Gal}(L_1/K)\cong\mathrm{Gal}(L_2/K)$.
(b) Let $L\colon K$ be a finite extension. Prove that $\mathrm{Gal}(L/K)$ is a finite group. Give examples to show that, if $L\colon K$ is infinite, then the Galois group may either be finite or infinite.

Solution:
(a) Take $K=\mathbb{Q}$. Then $L_1=\mathbb{Q}(\sqrt{2})$ and $L_2=\mathbb{Q}(\sqrt{3})$ satisfy the required properties.
(b) Let $K=\mathbb{Q}$. If $L=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\ldots)$, then $\mathrm{Gal}(L/K)$ is infinite. If $L=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3},\sqrt[3]{5},\ldots)$, then $\mathrm{Gal}(L/K)$ is trivial.

(4) Let L be a Galois extension of K such that $\mathrm{Gal}(L/K)\cong\mathbb{Z}_2\times\mathbb{Z}_{12}$. How many intermediate fields M are there such that (i) $[L\colon M]=4$, (ii) $[L\colon M]=9$, (iii) $\mathrm{Gal}(L/M)\cong\mathbb{Z}_4$?

Solution:
(a) By the fundamental theorem, we need to find the number of subgroups of $\mathbb{Z}_2\times\mathbb{Z}_{12}$ with 6 elements. There are three: $\langle(0,2)\rangle$, $\langle(1,2)\rangle$ and $\mathbb{Z}_2\times\langle 4\rangle$. Hence there are three intermediate fields M such that $[L\colon M]=4$.
(b) Since 9 does not divide 24, there are no such fields.
(c) We know that $\mathrm{Gal}(L/M)=M^*$, so we wish to count the number of subgroups of $\mathbb{Z}_2\times\mathbb{Z}_{12}$ that are isomorphic to $\mathbb{Z}_4$. There are two such subgroups: $\langle(0,2)\rangle$ and $\langle(1,2)\rangle$. Hence there are two intermediate fields M such that $\mathrm{Gal}(L/M)\cong\mathbb{Z}_4$.

(5) Let $K\subseteq M\subseteq L$ be fields. Prove or disprove.
(a) If $L\colon K$ is Galois, then $L\colon M$ is Galois.
(b) If $L\colon K$ is Galois, then $M\colon K$ is Galois.
(c) If $M\colon K$ and $L\colon M$ are Galois, then $L\colon K$ is Galois.

Solution:
(a) This statement is true by the Fundamental Theorem of Galois Theory.
(b) This statement is false. Consider $L=\mathbb{Q}(\sqrt[3]{2},e^{2\pi i/3})$, $M=\mathbb{Q}(\sqrt[3]{2})$ and $K=\mathbb{Q}$.
(c) This statement is false. Consider $L=\mathbb{Q}(\sqrt[4]{2})$, $M=\mathbb{Q}(\sqrt{2})$ and $K=\mathbb{Q}$.

(6) Find the Galois group of x^4-2 over (i) $\mathbb{Z}_3$ and (ii) $\mathbb{Z}_7$.

Solution:

(a) We have $x^4 - 2 = (x^2 + x + 2)(x^2 + 2x + 2)$ in $\mathbb{Z}_3[x]$. Since $\mathbb{F}_9$ is the splitting field of both $x^2 + x + 2$ and $x^2 + 2x + 2$, it is the splitting field of $x^4 - 2$. Hence the Galois group is $\mathbb{Z}_2$.
(b) We have $x^4 - 2 = (x + 2)(x + 5)(x^2 + 4)$ in $\mathbb{Z}_7[x]$. Hence the splitting field is $\mathbb{F}_{49}$ and the Galois group is $\mathbb{Z}_2$.

(7) (a) Using the fact that $\mathbb{F}_{p^n} : \mathbb{Z}_p$ is always Galois, show that, if $f \in \mathbb{Z}_p[x]$ is irreducible, then $\mathbb{Z}_p(\alpha)$ is the splitting field for f for any root α of f.
(b) Prove that, if $f \in \mathbb{F}_{p^m}[x]$ is irreducible, then f divides $x^{p^{mn}} - x$ iff the degree of f divides n.

Solution:
(a) Suppose that $\deg f = n$ and let α be a root of f. Then $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$, so $\mathbb{Z}_p(\alpha)$ is isomorphic to $\mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n} : \mathbb{Z}_p$ is Galois, we can conclude that $\mathbb{Z}_p(\alpha) \cong \mathbb{F}_{p^n}$ is the splitting field of f over $\mathbb{Z}_p$.
(b) Suppose that $f \in \mathbb{F}_{p^m}[x]$ is irreducible and has degree r. If f divides $x^{p^{mn}} - x$, then the $\mathbb{F}_{p^{mn}}$ contains $\mathbb{F}_{p^{mr}}$, the splitting field of f. Therefore $mr|mn$, or $r|n$. Now suppose that $r|n$. Then $\mathbb{F}_{p^{mr}}$, the splitting field of f, is contained in $\mathbb{F}_{p^{mn}}$. For every root α of f, we know that α is a root of $x^{p^{mn}} - x$, so f divides $x^{p^{mn}} - x$, as required.

(8) Let p and q be prime numbers. Prove that there are $\frac{p^{mq} - p^m}{q}$ irreducible polynomials $f \in \mathbb{F}_{p^m}[x]$ of degree q. (Hint: Use the previous problem.)

Solution: We know from the previous problem that f divides $x^{p^{mq}} - x$ iff the degree of f divides q. Therefore the irreducible divisors of $x^{p^{mq}} - x$ in $\mathbb{F}_{p^m}$ have degree q or 1. Let r be the number of irreducible polynomials of degree q in $\mathbb{F}_{p^m}[x]$. Clearly there are p^m irreducible (monic) polynomials of degree 1 in $\mathbb{F}_{p^m}[x]$. Therefore by comparing degrees, we have $p^{mq} = p^m + rq$, so $r = \frac{p^{mq} - p^m}{q}$.