Rowan Lochrin
MATH415B - Klaus Lux
4/22/18
Homework 10

1 Chapter 22

28 Draw the subfield lattice of $GF(3^{18})$ and of $GF(2^{30})$.

$$\begin{array}{ccc} & GF(3^{18}) & \\ \swarrow & & \searrow \\ GF(3^9) & & GF(3^2) \\ \downarrow & & \downarrow \\ GF(3^3) & & \downarrow \\ \searrow & & \swarrow \\ & GF(3) & \end{array} \qquad \begin{array}{ccc} & GF(2^{30}) & \\ \swarrow & \downarrow & \\ GF(2^2) & GF(3^{15}) & \\ \downarrow & \downarrow & \searrow \\ \downarrow & GF(3^3) & GF(3^5) \\ \searrow & \downarrow & \swarrow \\ & GF(3) & \end{array}$$

32 Let $f(x)$ be a cubic irreducible over Z_p, where p is a prime. Prove that the splitting field $f(x)$ over Z_p has order p^3 or p^6.

Proof. Let $f(a) = 0$ where $a \in E$, some extension field of Z_p, then in $Z_p(a)$, $f(x) = (x - a)g(x)$ where $g(x)$ is a degree two polynomial in $Z_p(a)$ if $g(x)$ is reducible then $f(x)$ splits completely in $Z_p(a)$ and because $Z_p(a) \approx Z_p[x]/ < f(x) >$, $|Z_p(a)| = p^3$. If $g(x)$ is not reducible in $Z_p(a)$, let $g(b) = 0$ where $b \in E$ then $f(x)$ splits completely in $Z_p(a)(b) = Z_p(a, b)$. Because $Z_p(a)(b) \approx Z_p(a)[x]/ < g(x) >$,$|Z_p[x]| = p^6$ $\square$

35 Suppose that F is a field of order 125 and $F^* =< \alpha >$. Show that $\alpha = -1$.
Because F is a finite filed $F^* \approx Z_{124}$. Because $< \alpha >= Z_{124}$, $\alpha^i = 1$ for some $i \leq 124$ if

$$\{\alpha^1, ..., \alpha^{124}\} = \{\alpha^1, ..., \alpha^{i-1}, 1, 1\alpha, ...\} = \{\alpha^1, ..., \alpha^i\} = Z_{124}$$

So $i = 124$ and $\alpha^{124} = (\alpha^{62})^2 = 1$ meaning $\alpha^{62} = 1$ or -1, and by the above it can't be the former.

2 Chapter 23

10 Prove that it is impossible to construct a $40°$ angle.

Proof. Note that construction a $40°$ angle would imply that you were also able to create a line of length $\cos 40°$. Consider the trig identity

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

Plugging in $40°$ can see that

$$0 = \cos^3 40° - 3\cos 40° + \frac{1}{2}$$

So $\cos 40°$ is a zero of the polynomial

$$8x^3 + 6x + 1$$

Meaning $[Q(\cos 40°) : Q] = 3$. So there cannot be a series of finite field extensions of degree 2 that include $\cos 40°$. $\square$

3 Chapter 32

5 Let E be an extension field of a field F and let H be a subgroup of $Gal(E/F)$. Show that the fixed field of H is indeed a field.
For all $\phi \in H$ if $\phi(a) = a$ and $\phi(b) = b$.

$$\begin{aligned}
\phi(a+b) &= \phi(a) + \phi(b) = a + b \\
\phi(a-b) &= \phi(a) - \phi(b) = a - b \\
\phi(ab) &= \phi(a)\phi(b) = ab \\
\phi(ab^{-1}) &= \phi(a)\phi(b)^{-1} = ab^{-1}
\end{aligned}$$

7 Let $f(x) \in F[x]$ and let the zeros of $f(x)$ be $a_1, a_2, ..., a_n$. If $K = F(a_1, a_2, ..., a_n)$, show that $Gal(K/F)$ is isomorphic to a group of permutations of the a_i's.
Because we know that all elements of F are fixed under $\phi \in Gal(K/F)$ so $\phi(0) = 0$, and

$$\begin{aligned}
\phi(p(a_i)) &= \phi(c_0 + c_1 a_i + c_2 a_i^2 + ... + c_n a_i^n) \\
&= \phi(c_0) + \phi(c_1 a_i) + \phi(c_2 a_i)^2 + ... + \phi(c_n a_i)^n \\
&= \phi(c_0) + \phi(c_1)\phi(a_i) + \phi(c_2)\phi(a_i^2) + ... + \phi(c_n)\phi(a_i^n) \\
&= c_0 + c_1\phi(a_i) + c_2\phi(a_i)^2 + ... + c_n\phi(a_i)^n \\
&= p(\phi(a_i)) = 0
\end{aligned}$$

Meaning that every member of $Gal(K/F)$ must send every a_i to another root of p. So every automorphism of $Gal(K/F)$ corresponds to a permutation of the a_i's.

10 Let $E = Q(\sqrt{2}, \sqrt{5})$. What is the order of the group $Gal(E/Q)$? What is the order of $Gal(Q\sqrt{10}/Q)$?
By the first part of the fundamental theorem of Galois theory, $[Q(\sqrt{2}, \sqrt{5}) : Q] = |Gal(Q(\sqrt{2}, \sqrt{5})/Q|$ and

$$[Q(\sqrt{2}, \sqrt{5}) : Q] = [Q(\sqrt{2}, \sqrt{5}) : Q(\sqrt{2})][Q(\sqrt{2}) : Q]$$

Clearly $[Q(\sqrt{2}) : Q] = 2$ we can see $\{1, \sqrt{5}, \sqrt{10}\}$ is a basis for $Q(\sqrt{2}, \sqrt{5})$ over $Q(\sqrt{2})$ so $[Q(\sqrt{2}, \sqrt{5}) : Q(\sqrt{2})] = 3$ meaning $|Gal(Q(\sqrt{2}, \sqrt{5})/Q| = 6$. Also $[Q(\sqrt{10}) : Q] = 2$ so $|Gal(Q(\sqrt{10})/Q| = 2$.

11 Suppose that F is a field of characteristic 0 and E is the splitting field for for some polynomial over F. If $Gal(E/F)$ is isomorphic to $Z_{20} \oplus Z_2$, determine the number of subfields L of E there are such that

1. $[L : F] = 4$.
   Because there is a one-to-one correspondence between subgroups fields of E containing F and the number of subgroups of $Gal(E/F)$ given by $L \to Gal(E/L)$ and because $[E : L] = |Gal(E/L)|$ we seek to find the number of subfields L such that $[E : F] = [E : L][L : F]$. By part one of the fundamental therome $[E : F] = |Gal(E/F)| = 40$ so we seek to find subfields L such that $[E : L] = 10$. So we need only to count the subgroups of $Z_{20} \oplus Z_2$ of order 10 to determine the the number of such subfields. There are 3 subgroups of $Z_{20} \oplus Z_2$ of order 10.
2. $[L : F] = 25$.
   By part one of the fundamental theorem of Galois theory $[L : F] = |Gal(E/F)|/|Gal(L/F)|$ because $|Gal(E/F)| = |Z_{20} \oplus Z_2| = 40$ clearly there is no integer n such that $25 = 40/n$ so there are no such subfields.
3. $Gal(E/L)$ is isomorphic to Z_5.
   There is only one subgroup of $Gal(E/F)$ isomorphic to Z_5.

16 Let p be a prime. Suppose that $|Gal(E/F)| = p^2$ draw all possible subfield lattices for fields between E and F.
For every subfield lattice between E and F there exists a corresponding subgroup lattice of $Gal(E/F)$ by lagrange's theorem the only possible subgroups of a group of order p^2 are of order p or 1. So the only three possible subfield lattices between F and E are one with p intermediate fields $P_1, ..., P_p$ such that $[P_i : F] = [E : P_i] = p$, one with one intermediate field P with $[P : F] = p$, and the one with no intermediate fields.