MATH 594, WINTER 2006, PROBLEM SET 7


Warm-up (not to be handed in)

[DF], §13.6, exercises 1–5, 16, §14.1, exercises 1–5, §14.2, exercises 1,2.

1. Exercises to be handed in

Exercise 1. Do [DF], §13.6, exercise 6.

Solution. Suppose that \( \zeta_n \) is a primitive \( n \)-th root of unity. Suppose that \( (-\zeta_n)^b = 1 \). Then \( \zeta_n^{2b} = 1 \) and \( n \) divides \( 2b \). Since \( n \) is odd, \( n \) divides \( b \). But \( (-\zeta_n)^n = -1 \) because \( n \) is odd. Therefore, the order of \( (-\zeta_n) \) is \( 2n \). So \( -\zeta_n \) is a primitive \( 2n \)-th root of unity. \( \Phi_n(x) \) is the minimum polynomial of \( \zeta_n \). So \( \Phi_n(-x) \) is the minimum polynomial of \( -\zeta_n \). It follows that \( \Phi_n(-x) = \Phi_{2n}(x) \). 


Solution. Suppose that \( \sigma \) is an automorphism of \( k(t) \) over \( k \). Then we can write \( \sigma(t) = \frac{p(t)}{q(t)} \) where \( p(t) \) and \( q(t) \) are relatively prime. The polynomial \( q(t)s - p(t) \) is irreducible as a polynomial in \( t \) and \( s \) if \( q(t)s - p(t) \) factors, then one of the polynomial factors is a polynomial in \( t \). But \( q(t) \) and \( p(t) \) do not have a common factor, so this factor must be constant. Since \( q(t)s - p(t) \) is irreducible as a polynomial in \( s \) and \( t \) it is irreducible as a polynomial in \( t \) by Gauss’ Lemma. If \( d \) is the maximum of the degrees of \( q(t) \) and \( p(t) \), then \( [\mathbb{Q}(t) : \mathbb{Q}(s)] = d \). If \( \sigma \) is an automorphism, then we must have \( \mathbb{Q}(s) = \mathbb{Q}(t) \) and \( d = 1 \). In other words, \( p(t) \) and \( q(t) \) are linear or constant. We can write

\[
\sigma(t) = \frac{at + b}{ct + d}.
\]

Clearly \( ad - bc \neq 0 \) otherwise \( \sigma(t) \) is a constant.

Conversely, if \( ad - bc \neq 0 \) then

\[
\sigma(t) = \frac{at + b}{ct + d}
\]

defines an automorphism where the inverse \( \sigma^{-1} \) is given by

\[
\sigma^{-1}(t) = \frac{dt - b}{-ct + a}.
\]

Solution. We already have seen that \([Q(\sqrt{2}, \sqrt{3}) : Q] = 4\) (see §13.2, page 526). Similarly \([Q(\sqrt{2}, \sqrt{5}) : Q] = 4\), \([Q(\sqrt{3}, \sqrt{5}) : Q] = 4\) and \([Q(\sqrt{6}, \sqrt{5}) : Q] = 4\). Suppose that \(\sqrt{5} \in Q(\sqrt{2}, \sqrt{3})\). Then \(Q(\sqrt{5})\) is one of the fields \(Q(\sqrt{2}), Q(\sqrt{3}), Q(\sqrt{6})\) but \([Q(\sqrt{2}, \sqrt{5}) : Q] = 4\), \([Q(\sqrt{3}, \sqrt{5}) : Q] = 4\) and \([Q(\sqrt{6}, \sqrt{5}) : Q] = 4\). Contradiction. Therefore \(\sqrt{5} \not\in K := Q(\sqrt{2}, \sqrt{3}, \sqrt{5})\) and \([Q(\sqrt{2}, \sqrt{3}, \sqrt{5}) : Q] = 8\). Each element of the Galois group sends \(\sqrt{2}\) to \(\pm \sqrt{2}\), \(\sqrt{3}\) to \(\pm \sqrt{3}\) and \(\sqrt{5}\) to \(\pm \sqrt{5}\). Since the Galois group has 8 elements, each of these 8 possibilities defines an automorphism. Let \(\sigma_1, \sigma_2, \sigma_3\) be generators of the Galois group defined by

\[
\begin{align*}
-\sigma_1(\sqrt{2}) &= \sigma_2(\sqrt{2}) = \sigma_3(\sqrt{2}) = \sqrt{2} \\
\sigma_1(\sqrt{3}) &= -\sigma_2(\sqrt{3}) = \sigma_3(\sqrt{3}) = \sqrt{3} \\
\sigma_1(\sqrt{5}) &= \sigma_2(\sqrt{5}) = -\sigma_3(\sqrt{5}) = \sqrt{5}
\end{align*}
\]

The Galois group is \(Z_2 \times Z_2 \times Z_2\). We list all subgroups and using the Galois correspondence this gives all intermediate fields:

\[
\begin{align*}
K^{(\sigma_1)} &= Q(\sqrt{3}, \sqrt{5}), K^{(\sigma_2)} = Q(\sqrt{2}, \sqrt{5}), K^{(\sigma_3)} = Q(\sqrt{2}, \sqrt{3}), K^{(\sigma_1 \sigma_2)} = Q(\sqrt{6}, \sqrt{5}) \\
K^{(\sigma_1 \sigma_3)} &= Q(\sqrt{3}, \sqrt{10}), K^{(\sigma_2 \sigma_3)} = Q(\sqrt{2}, \sqrt{15}), K^{(\sigma_1 \sigma_2 \sigma_3)} = Q(\sqrt{6}, \sqrt{10}) \\
K^{(\sigma_2 \sigma_1 \sigma_3)} &= Q(\sqrt{5}), K^{(\sigma_2, \sigma_3)} = Q(\sqrt{3}), K^{(\sigma_2, \sigma_2 \sigma_3)} = Q(\sqrt{2}), K^{(\sigma_1, \sigma_2 \sigma_3)} = Q(\sqrt{15}), K^{(\sigma_2, \sigma_1 \sigma_2 \sigma_3)} = Q(\sqrt{10}), K^{(\sigma_3, \sigma_1 \sigma_2)} = Q(\sqrt{6}), K^{(\sigma_1 \sigma_2 \sigma_2 \sigma_3)} = Q(\sqrt{30}).
\end{align*}
\]


Solution. Let \(E\) be the splitting field of \(x^p - 2\). Then \(E\) is generated by \(p\sqrt{2}\) and \(\zeta_p\) where \(\zeta_p\) is a primitive \(p\)-th root of unity. \([Q(\zeta_p) : Q] = p - 1\) and \([Q(p\sqrt{2}) : Q] = p\) (because \(x^p - 2\) is irreducible). It follows that \([K : Q] \leq p(p - 1)\) where \(K = Q(\zeta_p, p\sqrt{2})\). Also \([K : Q]\) is divisible by \(p\) and \(p - 1\). We conclude that \([K : Q] = p(p - 1)\). The Galois group has \(p(p - 1)\) elements. If \(\sigma\) is an element of the Galois group, then \(\sigma\) sends \(p\sqrt{2}\) to \(\zeta^i p\sqrt{2}\) for some \(i\) (because all roots of \(x^p - 2\) are of this form) and sends \(\zeta\) to \(\zeta^j\) (with \(1 \leq j \leq p - 1\)). Each of the \((p - 1)p\) possibilities must define an automorphism. Let \(\sigma\) be the automorphism of order \(p\) defined by \(p\sqrt{2} \mapsto \zeta^i p\sqrt{2}\) and \(\zeta \mapsto \zeta\). Let \(\tau\) be the automorphism of order \(p - 1\) defined by \(p\sqrt{2} \mapsto 2\sqrt{2}\) and \(\zeta \mapsto \zeta^a\) where \(a\) generates the multiplicative group \(\mathbb{F}_p^*\). Then \(\tau\sigma\tau^{-1} = \sigma^a\). This shows that the Galois group is a semidirect product \(Z_{p-1} \rtimes Z_p\).


Solution. We look at the example on page 577. The Galois group is generated by \(\sigma\) and \(\tau\) with \(\sigma^8 = \tau^2 = 1\) and \(\tau\sigma\tau^{-1} = \sigma^3\). The (nontrivial) normal subgroups are:

\[
\langle \sigma \rangle, \langle \sigma^2 \rangle, \langle \sigma^4 \rangle, \langle \tau, \sigma^2 \rangle, \langle \tau \sigma, \sigma^2 \rangle.
\]
Using the Galois correspondence, we get the following fields:

\[ Q(i), Q(i, \sqrt{2}), Q(i, \sqrt{4\sqrt{2}}), Q(\sqrt{2}), Q(\sqrt{-2}). \]

**Hard Exercises (optional, for extra credit)**

**Exercise 6.** Do §13.6, 14–17.

HARM DERKSEN, 3067EH, 763 2309
Office hours: **MWF 3-4pm.**
http://www.math.lsa.umich.edu/~hderksen/math594.w06/index.html