Solutions to Homework 12
Math 601, Spring 2008

Exam II problems

1) a) For any automorphism from \( f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3}) \), \( f(\sqrt{2}) \) must be a root of \( X^2 - 2 \), in other words \( f(\sqrt{2}) = \pm \sqrt{2} \). But it is easy to check that \( \pm \sqrt{2} \notin \mathbb{Q}(\sqrt{3}) \).

b) As mentioned above \( \sqrt{2} \notin \mathbb{Q}(\sqrt{3}) \), thus \( |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| = 2 \cdot 2 = 4 \).

c) \( \sqrt{2} + \sqrt{3} \) is a primitive generator for \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) because it has 4 Galois conjugates under the Galois group \( (\sqrt{2}, \sqrt{3}) \leftrightarrow (\pm \sqrt{2}, \pm \sqrt{3}) \).

2) a) Let \( E = F(\alpha) \) with \( [E : F] = 2 \), then \( E \) is the splitting field of the irred. polynomial over \( F \) of \( \alpha \), thus \( E \) is normal by Problem 44), HW10.

b) Let \( F \subset K \subset L \) be \( \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{1 + \sqrt{2}}) \). By part a) \( K/F \) and \( L/K \) are normal, but if \( L/F \) were normal, it would be Galois (since we are in char. zero) contradicting Problem 49) HW11 according to which the Galois closure of \( L/F \) is \( L(i) \) or equivalently \( L(\sqrt{1 - \sqrt{2}}) \).

3) a) Let \( \Phi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p \) be the Frobenius automorphism. Then \( \mathbb{F}_{p^n} \) is the fixed field of the group of automorphisms \( \langle \Phi^n \rangle \). Thus \( \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} \) is the fixed field of \( \langle \Phi^n, \Phi^m \rangle = \langle \Phi^{(m,n)} \rangle \) where \( (m, n) \) is the gcd of \( m \) and \( n \). Thus \( \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{\gcd(m,n)}} \).

b) \( \alpha \) has order 5 in \( \mathbb{F}_{p^n} = \mathbb{Z}/(p - 1)\mathbb{Z} \) and thus \( p \equiv 1 \mod 5 \).

4) Let \( E/\mathbb{Q} \) be the splitting fld. of \( X^5 + 2 \). We will show \([E : \mathbb{Q}] = 5 \cdot 4 = 20\) as a particular case of the following claim:

Claim: Let \( E/\mathbb{Q} \) be the splitting field of \( X^p - n \), where \( p \) is a prime and \( n \in \mathbb{Z} \) is not a \( p \)-th power, then \([E : \mathbb{Q}] = p \cdot (p - 1)\).

Proof: Let \( \xi = \xi_p \) be a primitive \( p \)-th root of unity. We have \([E : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] [E : \mathbb{Q}(\xi)] = (p - 1)[E : \mathbb{Q}(\xi)] \). Observe that \( E/\mathbb{Q}(\xi) \) is Galois, and \( \text{Gal}(E/\mathbb{Q}(\xi)) \) is a subgroup of the group of permutations of the roots \( \{n^{1/p} \xi^i \mid 1 \leq i \leq p\} \) and fixing \( \xi \), i.e., \( \text{Gal}(E/\mathbb{Q}(\xi)) \) is a subgroup of the cyclic group \( \mathbb{Z}/p\mathbb{Z} \) generated by \( n^{1/p} \mapsto n^{1/p} \xi \). Thus we only need to show that \( \text{Gal}(E/\mathbb{Q}(\xi)) \) is not
trivial, i.e. that \( E \neq \mathbb{Q}(\xi) \). Indeed, if \( E = \mathbb{Q}(\xi) \), then \( [E : \mathbb{Q}] = p - 1 \) implies \( p \nmid [E : \mathbb{Q}] \) and hence \( X^p - n \) must be reducible over \( \mathbb{Q} \). We show two ways to prove that \( X^p - n \) is irreducible (assuming \( n \) is not a \( p \)-th power):

i) If \( E = \mathbb{Q}(\xi) \), then \( \text{Gal}(E/\mathbb{Q}) = \mathbb{Z}/(p - 1)\mathbb{Z} \) is abelian and hence any intermediate extension \( F/\mathbb{Q} \) with \( \mathbb{Q} \subset F \subset E \) is Galois. Suppose \( X^p - n \) is reducible and let \( F = \mathbb{Q}(\alpha) \) where \( \alpha \) is a root of an irreducible factor \( f(X) \) of \( X^p - n \) of degree \( 2 \leq m \leq p - 2 \). (If \( m = 1 \) or \( p - 1 \) then \( X^p - n \) has a linear factor, i.e \( n \) is a \( p \)-th power). Since \( F/\mathbb{Q} \) is Galois and \( f(X) \) is an irreducible polynomial, it splits completely in \( F \). This implies \( \xi \in F \) because \( m \geq 2 \) and the roots of \( f(X) \) in \( E \) are \( \{\alpha \xi^i\} \). Thus \( F = \mathbb{Q}(\xi) \), but then \( m = [F : \mathbb{Q}] = p - 1 \) contradicting \( 2 \leq m \leq p - 2 \).

ii) We showed in the Proposition in the solution of Problem 32, HW7 without explicitly using Galois theory, that \( X^p - n \) is irreducible if \( n \) is not a \( p \)-th power.

5) Show that \( G := \text{Gal}(X^3 - 2) = S_3 \). Let \( K \) be the splitting field in question. Clearly \( |G| = [E : \mathbb{Q}] \leq 3 \cdot 2 = 6 \). \( H := \text{Gal}(K/\mathbb{Q}(\xi_3)) \) is a nontrivial subgroup of the cyclic group of order 3 generated by \( 2^{1/3} \mapsto 2^{1/3}\xi_3 \) and hence equal to it. (If \( |H| = 1 \) then \( E = \mathbb{Q}(\xi_3) \), again implying \( X^3 - 2 \) reducible, which implies \( 2^{1/3} \in \mathbb{Q} \)). Similarly \( K := \text{Gal}(E/\mathbb{Q}(2^{1/3})) \) is cyclic of order 2 generated by \( \xi_3 \mapsto \xi_3^{-1} \). It is easy to check that \( HK < G \) is \( S_3 \), hence \( G = S_3 \).

b) The quadratic extension of \( Q \) in question is \( Q(\xi_3)/\mathbb{Q} \).

6) The cyclotomic extension \( Q(\xi)/\mathbb{Q} \) is a simple extension of degree \( \phi(n) \), the irreducible polynomial of \( \xi = \xi_n \) being the \( n \)-th cyclotomic polynomial \( \Phi_n(X) \). The roots of the \( \Phi_n(X) \) in \( Q(\xi) \) are the primitive roots of unity (by definition). It follows that the \( \text{Gal}(Q(\xi)/\mathbb{Q}) \) consists of the automorphisms \( \xi \mapsto \xi^i \) such that \( \xi^i \) is a primitive root of unity. Thus \( \text{Gal}(Q(\xi)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times \).

7) Let \( G \hookrightarrow S_n \) be a monomorphism. We have a Galois extension \( Q(s_1, \ldots, s_n) \subset Q(X_1, \ldots, X_n) =: K \) with Galois group \( S_n \), where the \( s_i \) are the elementary symmetric polynomials in \( [X_1, \ldots, X_n] \). Let \( Q(s_1, \ldots, s_n) \subset F \subset K \) be the intermediate field corresponding to \( G \subset S_n \). We thus have a Galois extension \( K/F \) with Galois group \( G \), and we can find an intermediate field \( F \subset E \subset K \) with \( \text{Gal}(K/E) = H \) and \( \text{Gal}(E/F) = G/H \).

HW 12 problems, Section 18.1 [D-F]
55) [D-F] 18.1 #6 (10 points). It is straight-forward to write down the matrices.

56) [D-F] 18.1 #8 (10 points). \( \sigma \cdot v = v \) forces the entries of \( v \) to be identical, thus \( v = v_0 := \sum_i e_i \). For the same reason \( V \) has a unique one dimensional submodule \( (n \geq 3) \), namely \( Fv_0 \).

57) [D-F] 18.1 #13 (10 points). a) If \( M, N \) are simple \( R \)-modules and \( f : M \to N \) a nontrivial \( R \)-module homomorphism, then \( \ker(f) \neq M \) and \( \text{im}(f) \neq 0 \), whence \( \ker(f) = 0 \) and \( \text{im}(f) = N \). In other words \( f \) is an isomorphism.

b) by part a) every element of \( \text{Hom}_R(M, M) \) has a two-sided inverse, which makes it into a division ring.

58) [D-F] 18.1 #18 (10 points). Let \( \lambda \in \mathbb{C} \) be an eigenvalue of the matrix \( A \) with eigenspace \( W \subset \mathbb{C}^n \). Since \( A \) commutes with \( \phi(g) \) for all \( g \), it follows that \( W \) is \( G \)-invariant subspace of positive dimension, and hence \( W = \mathbb{C}^n \). Thus \( A = \lambda I \). In particular, \( \phi \) restricts to a homomorphism \( \hat{\phi} : Z(G) \to \mathbb{C}^\times \). Since any finite subgroup of the multiplicative group of a field is cyclic, \( \text{im}(\hat{\phi}) \) is cyclic. If \( \phi \) is faithful then, it follows that \( Z(G) \) is cyclic, and \( \phi(z) \) is a scalar matrix for all \( z \in Z(G) \).