Math 504, Fall 2013
HW 3

1. Using only the fact that $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$, show that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ whenever m divides n.

Suppose $n = mk$ for some $k \in \mathbb{N}$. We know that $\mathbb{F}_{p^m}$ is the splitting field of $x^{p^m} - x$ and thus every $\alpha \in \mathbb{F}_{p^m}$ satisfies $\alpha^{p^m} = \alpha$. Thus to show $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^{mk}}$, it suffices to show that every $\alpha \in \mathbb{F}_{p^m}$ also satisfies

$$\alpha^{p^{mk}} = \alpha. \tag{1}$$

In terms of the Frobenius automorphism $\sigma(\beta) := \beta^p$, (1) says that $\sigma^{mk}(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_{p^m}$. We prove this holds for any $k \in \mathbb{N}$ by induction. We already saw above that the case $k = 1$ holds. Let $\ell \in \mathbb{N}$ and suppose $\sigma^{m\ell}(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_{p^m}$. Then for any $\alpha \in \mathbb{F}_{p^m}$,

$$\sigma^{m(\ell+1)}(\alpha) = \sigma^m\big(\sigma^{m\ell}(\alpha)\big) = \sigma^m(\alpha) = \alpha^{p^m} = \alpha,$$

proving the claim. Thus $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^{mk}}$ for all $k \in \mathbb{N}$. ∎

2. Let $\xi = \xi_p$. Let $R = \{\xi^i \mid i \in \mathbb{Z}\}$. Show that R is a ring with the operations

$$\xi^i \oplus \xi^j = \xi^{i+j} \qquad \text{and} \qquad \xi^i \odot \xi^j = \xi^{ij}.$$

Show that $R \cong \mathbb{F}_p$.

We first show that R is a ring. We go through the details, even though it is somewhat obvious that R inherits the ring structure of $\mathbb{Z}$.

Clearly $\oplus$ is commutative and for any $n \in \mathbb{Z}$, $\xi^n \oplus \xi^0 = \xi^{n+0} = \xi^n$, and so ξ^0 is the additive identity. Also, $\xi^n \oplus \xi^{-n} = \xi^0$, and so R is an abelian group under $\oplus$.

If $\ell, m, n \in \mathbb{Z}$, then using the associativity of multiplication in $\mathbb{Z}$, we find

$$(\xi^\ell \odot \xi^m) \odot \xi^n = \xi^{\ell m} \odot \xi^n = \xi^{\ell m n} = \xi^\ell \odot \xi^{mn} = \xi^\ell \odot (\xi^m \odot \xi^n),$$

and so multiplication is associative (as well as clearly being commutative). Furthermore,

$$\xi^\ell \odot (\xi^m \oplus \xi^n) = \xi^\ell \odot \xi^{m+n} = \xi^{\ell(m+n)} = \xi^{\ell m + \ell n} = \xi^{\ell m} \oplus \xi^{\ell n} = (\xi^\ell \odot \xi^m) \oplus (\xi^\ell \odot \xi^n).$$

Distribution from the right also follows from right distribution among the integers. ∎

3. Let p be a prime number. Let $\xi_p = e^{2\pi i/p}$ and $K = \mathbb{Q}(\xi)$. Show there is a group homomorphism $\Phi : \text{Gal}\,(K/\mathbb{Q}) \to \text{Aut}(R)$, the automorphism group of R. Deduce that $\text{Gal}\,(K/\mathbb{Q}) \cong \mathbb{F}_p^\times$, the multiplicative group of p^{th} roots of unity. Deduce that Gal $(K/\mathbb{Q})$ is the cyclic group of order $p-1$.

Let p be prime with $\xi = \xi_p$ and $K = \mathbb{Q}(\xi)$. Then K is the splitting field of the pth cyclotomic polynomial $\Phi_p(x)$ (of degree $p-1$) over $\mathbb{Q}$, hence $K/\mathbb{Q}$ is a Galois extension. Elements of $G = \text{Gal}\,(K/\mathbb{Q})$ are automorphisms of K that fix $\mathbb{Q}$, hence they are completely determined by where they send ξ. The Galois group permutes the roots of $\Phi_p(x)$, so the distinct possibilities are ξ^i for $1 \leq i \leq p-1$. Since $[K/\mathbb{Q}] = p-1$, each one of these is an element of the Galois group. We will label the elements of Gal $(K\mathbb{Q})$ as σ_i, where $\sigma_i(\xi) = \xi^i$.

Now we consider group automorphisms under $\oplus$ of the group R above. We see that the element ξ generates R under the $\oplus$ operation. Each automorphism must fix the identity element $\xi_0 = 1$ and is then completely determined by the image of ξ. In order to be an automorphism, the image of ξ must also generate R under $\oplus$; the generators are ξ^i for $1 \leq i \leq p-1$, so each of these gives a valid and distinct automorphism. Denote by τ_i the automorphism defined by $\tau_i(\xi) = \xi^i$.

Now we'll write a map $\Psi : \text{Gal}\,(K/\mathbb{Q}) \to \text{Aut}\,(R)$ defined by $\Psi(\sigma_i) = \tau_i$. The operation of composition clearly carries through Ψ, so this is a group homomorphism. The identity automorphism τ_1 is uniquely the image of σ_1, the identity automorphism of G. Hence, Ψ is injective. Each τ_i is the image of σ_i because the range of i is the same in both cases. Hence, we have an isomorphism between Gal $(K/\mathbb{Q})$ and Aut (R).

From the result of problem **(2)**, we also conclude that Gal $(K/\mathbb{Q})$ is isomorphic to the group of automorphisms of $\mathbb{F}_p$ under addition. This is the same of the automorphisms of $\mathbb{Z}_p$. For a general $n \in \mathbb{Z}$, the automorphism group of $\mathbb{Z}_n$ is isomorphic to the group of units $\mathbb{Z}_n^\times$. This group is isomorphic to $\mathbb{Z}_{\varphi(n)}$ where φ is Euler's totient function. Hence, in our case we have $\text{Gal}\,(K/\mathbb{Q}) \cong \mathbb{F}_p^\times \cong \mathbb{Z}_{p-1}$ and this tells us that Gal $(K/\mathbb{Q})$ is the cyclic group of order $p-1$. ■

4. Let p be an odd prime and $\xi_p = e^{2\pi i/p}$. Explain why there is a field F such that $\mathbb{Q} \subset F \subset \mathbb{Q}(\xi_p)$ and $[F : \mathbb{Q}] = 2$. Why is $F = \mathbb{Q}(\sqrt{d})$ for some d? Find d.

The field $\mathbb{Q}(\xi_p)$ is the splitting field of the pth cyclotomic polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. The roots of this polynomial are the primitive pth roots of unity ξ_p^k for $1 \leq k \leq p-1$. The discriminant $\Delta(f)$ of f is defined to be:

$$\Delta(f) = \prod_{1 \leq i < j \leq p-1} (\xi_p^i - \xi_p^j)^2$$

The Galois group $G = \text{Gal}\,(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is a group of permutations that acts on the roots of f. If we permute the roots in the list of terms $(\xi_p^i - \xi_p^j)$, we end up with the same list except for a negative sign on some terms. If we are squaring every term, then we end up with exactly the same value. Said another way, $\Delta(f)$ is fixed by every element in the Galois group. Since this is a Galois extension, $\Delta(f)$ must be an element of $\mathbb{Q}$.

Now consider the square root of the discriminant:

$$\sqrt{\Delta(f)} = \prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)$$

This is an element of $\mathbb{Q}(\zeta_p)$, certainly, but it may or may not be an element of $\mathbb{Q}$.

By the proof of Prop. 9.50 in the textbook we have

$$\Delta(f) = \det \begin{bmatrix} p-1 & a_1 & \dots & a_{p-2} \\ a_1 & a_2 & \dots & a_{p-1} \\ a_2 & a_3 & \dots & a_p \\ & & \vdots & \\ a_{p-2} & a_{p-1} & \dots & a_{2p-4} \end{bmatrix}$$

Now $a_p = \sum_{i=1}^{p-1} \zeta^{ip} = \sum_{i=1}^{p-1} 1^i = p-1$. The a_i go up to $2p-4 < 2p$, so every other index is relatively prime to p. For those a_j (those where $j \neq p$):

$$a_j = \sum_{i=1}^{p-1} \zeta^{ij} = \sum_{i \in \mathbb{F}_p^\times} \zeta^{ij} = \sum_{k=ij \in \mathbb{F}_p^\times} \zeta^k = -1$$

That is, every other entry of the matrix is -1:

$$\Delta(f) = \det \begin{bmatrix} p-1 & -1 & \dots & -1 \\ -1 & -1 & \dots & -1 \\ -1 & -1 & \dots & p-1 \\ & & \vdots & \\ -1 & -1 & \dots & -1 \end{bmatrix} = \det \begin{bmatrix} p & 0 & 0 & \dots & 0 \\ -1 & -1 & -1 & \dots & -1 \\ 0 & 0 & 0 & \dots & p \\ & & & \vdots & \\ 0 & 0 & p & \dots & 0 \end{bmatrix}$$

Note that I subtracted the second row from every other row to get the equality. By the recursive definition of the determinant:

$$\Delta(f) = p \det \begin{bmatrix} -1 & -1 & \dots & -1 \\ 0 & 0 & \dots & p \\ & & \vdots & \\ 0 & p & \dots & 0 \end{bmatrix} = -p \det \begin{bmatrix} 0 & 0 & \dots & p \\ & & \vdots & \\ 0 & p & \dots & 0 \\ p & 0 & \dots & 0 \end{bmatrix}$$

Note that the matrix above is $(p-3) \times (p-3)$. The final determinant is $p^{p-3}\mathrm{sgn}((1, p-3)(2, p-4)...)$. There are exactly $\frac{p-3}{2}$ transpositions in that permutation, so the determinant of the most recent matrix is $(-1)^{\frac{p-3}{2}} p^{p-3}$, and overall, $\Delta(f) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

If we again use the notation $2r+1 = p$, then

$$\sqrt{\Delta(f)} = \sqrt{(-1)^{\frac{p-1}{2}} p^{2(r-1)+1}} = p^{r-1} \sqrt{(-1)^{\frac{p-1}{2}} p}$$

Thus we see that $F = \mathbb{Q}(\sqrt{p})$ if $p \cong 1 \mod 4$, $F = \mathbb{Q}(\sqrt{-p})$ if $p \cong 3 \mod 4$.

■

5. Take $p = 17$ above. Find all fields F such that $\mathbb{Q} \subset F \subset \mathbb{Q}(\zeta_p)$. Each intermediate field is of the form $\mathbb{Q}(\alpha)$ for some α. Can you find a nice α for each F?

Let $\zeta = \zeta_{17}$. Let $K = \mathbb{Q}(\zeta)$, and let $G = \text{Gal}\,(K/\mathbb{Q})$. We have $\text{Gal}\,(K/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^\times \cong C_{16}$, the cyclic group of 16 elements by problem 3. The elements $\{1, \zeta, \zeta^2, \ldots, \zeta^{15}\}$ form a basis for $K/\mathbb{Q}$. But since $1 + \zeta + \ldots + \zeta^{16} = 0$, the elements $\{\zeta, \zeta^2, \ldots, \zeta^{15}, \zeta^{16}\}$ also form a $\mathbb{Q}-$basis for K. It follows that elements $\sigma \in G$ permute these basis elements, as these are the primitive 17th roots of unity. We may use the $\mathbb{Q}-$basis for K consisting of the elements

$$\mathcal{B} = \{\zeta, \zeta^2, \ldots, \zeta^{16}\}$$

and any $\sigma \in G$ simply permutes these basis elements. Following page 597 of Dummit & Foote, if $H \leq G$ is a subgroup, then

$$\alpha_H = \sum_{\sigma \in H} \sigma(\zeta)$$

is the sum of the Galois conjugates of ζ as automorphisms range over H. For any $\tau \in H$, the elements $\tau\sigma$ run over the elements of H as σ runs through H, whence $\tau\alpha = \alpha$, so that $\alpha \in \mathbb{Q}^H$. However, if $\tau \notin H$, then $\tau\alpha$ is the sum of basis elements given above. If it were the case that $\tau\alpha = \alpha$ (so that $\alpha \in \mathbb{Q}$ as it is now fixed by all automorphisms), then since these elements are a basis, we must have $\tau(\zeta) = \sigma(\zeta)$ for one of the terms $\sigma\zeta$ appearing in the definition of α. But then then it would follow that $\tau\sigma^{-1} = 1$, the identity automorphism for this particular $\sigma \in H$, whence $\tau \in H$, a contradiction. This shows that α is not fixed by any automorphism not contained in H, so that $\mathbb{Q}(\alpha) = K^H$.

A generator for the cyclic subgroup $G \cong C_{16}$ is given by an automorphism σ mapping $\zeta \mapsto \zeta^3$, by order considerations. There are precisely three nontrivial subgroups of C_{16} : C_2, C_4, and C_8, and we compute α for various subgroups $H = C_j, j = 2, 4, 8$, and in the notation of $G = \langle\sigma\rangle, C_j = \langle\sigma^{16/j}\rangle$.

$$\alpha_2 = \zeta + \sigma^8(\zeta) = \zeta + \zeta^{3^8} = \zeta + \zeta^{16} = \boxed{\zeta + \zeta^{-1}}$$

$$\alpha_4 = \zeta + \sigma^4(\zeta) + \sigma^8(\zeta) + \sigma^{12}(\zeta) = \zeta + \zeta^{3^4} + \zeta^{3^8} + \zeta^{3^{12}} = \boxed{\zeta + \zeta^{13} + \zeta^{-1} + \zeta^4}$$

$$\alpha_8 = \zeta + \sigma^2\zeta + \sigma^4\zeta + \sigma^6\zeta + \sigma^8\zeta + \sigma^{10}\zeta + \sigma^{12}\zeta + \sigma^{14}\zeta = \boxed{\zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2}$$

■

6. Let $K/\mathbb{Q}$ be the splitting field of an irreducible polynomial of degree 3 and suppose that $\text{Gal}\,(K/\mathbb{Q})$ is the symmetric group S_3. Does K contain the three cube roots of 1? Explain.

Let $K/\mathbb{Q}$ be the splitting field of an irreducible polynomial $f(x)$ of degree 3 and suppose that $\text{Gal}\,(K/\mathbb{Q})$ is the symmetric group S_3. Since the Galois group is not contained in the alternating group A_n, the discriminant of $f(x)$ is not a square in $\mathbb{Q}$ and there is a non-trivial quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. This must be in correspondence with an index-2 subgroup of S_3 and there is only one such subgroup; namely, A_n.

If K contains all of the cube roots of unity, then K contains a subfield that is the splitting field of x^2+x+1 (the quadratic whose roots are the primitive cube roots of unity). This is a degree 2 extension, so we now see that if K contains all of the cube roots of unity, the fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\xi_3)$ must be equal as the unique quadratic extension of $\mathbb{Q}$ contained in K.

We will show that it is not true in general that K contains ξ_3 by providing a counterexample. Let $f(x) = x^3+2x+2$. This is irreducible by Eisenstein's criterion. Its discriminant is $D = -4(2)^3 - 27(2)^2 = -140$. This is factored as $-4(35)$, which is not a square in $\mathbb{Q}$. The only possible Galois groups of irreducible cubics are S_3 or A_3, as these are the only transitive subgroups of S_3. Since $\sqrt{D}$ is not in $\mathbb{Q}$, the Galois group is not contained in A_3 and it must be all of S_3. Hence, we are in the situation set out above.

The field $\mathbb{Q}(\xi_3)$ is realized as $\mathbb{Q}(\sqrt{-3})$, as $\xi_3 = \frac{1}{2} + i\sqrt{3}/2$. As proved before, if the splitting field of $f(x)$ contains the cube roots of unity then it must be that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{-35}$. Suppose that this is the case; every element in the second field can be written in the form $p+q\sqrt{-35}$ for some $p,q\in\mathbb{Q}$. Then there exists p,q such that:

$$\sqrt{-3} = p+q\sqrt{-35}$$
$$(\sqrt{-3})^2 = (p+q\sqrt{-35})^2$$
$$-3 = p^2 - 35q^2 + 2pq\sqrt{-35}$$

This is a contradiction, as it implies that $\sqrt{-35}$ is an element of $\mathbb{Q}$. Hence, it is not true in general that the splitting field of an irreducible polynomial with Galois group S_3 contains the cube roots of unity. ∎

7. Show that $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$ where α is a primitive 5^{th} root of 1 over $\mathbb{F}_2$.

We have that the minimal polynomial of α in $\mathbb{F}_2$ is $p(x) = 1+x+x^2+x^3+x^4$: irreducibility can be checked directly, since there are not many irreducible polynomials of small degree over $\mathbb{F}_2$.

Moreover, we know that $p(x)|x^{16}-x$. Since $\mathbb{F}_{16}$ is a splitting field for $x^{16}-x$, $\alpha\in\mathbb{F}_{16}$. Now, since $[\mathbb{F}_2(\alpha):\mathbb{F}_2] = 4$ it follows that $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$. Since $\mathbb{F}_4/\mathbb{F}_2$ is a degree two extension, $\alpha\notin\mathbb{F}_4$, and the containment $\mathbb{F}_4\subseteq\mathbb{F}_{16}$ gives us that $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$.

∎

8. If $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$ where α is a primitive 5^{th} root of 1 over $\mathbb{F}_2$ is there an element $\sigma \in \mathrm{Gal}\,(\mathbb{F}_16/\mathbb{F}_4)$ such that $\sigma(\alpha) = \alpha^2$? What about $\sigma(\alpha) = \alpha^3$?

The answer is no. The Frobenius automorphism $F : x \mapsto x^2$ is a generator of $G = \mathrm{Gal}\,(\mathbb{F}_{16}/\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$, as one can verify directly. Since $\mathbb{F}_4$ is the splitting field of x^4-x, then $F^2(x) = x^4 = x$ for all $x\in\mathbb{F}_4$ one can see that F^2 fixes $\mathbb{F}_4$ hence $\mathrm{Gal}\,(\mathbb{F}_{16}/\mathbb{F}_2)$ is cyclic of order two, generated by F^2. Therefore the only Galois conjugates of α are α and $\alpha^4 = \alpha^{-1}$, and none of them is equal to α^2 or α^3. ∎