SOLUTIONS TO WORKSHEET #7

Problem 1. — *Let n be any positive integer and let $\Phi_n(x) \in \mathbf{C}[x]$ denote the n-th cyclotomic polynomial; that is, the monic polynomial whose roots are exactly the primitive n-th roots of unity in $\mathbf{C}$. Prove that $\Phi_n(x) \in \mathbf{Z}[x]$ and that $\Phi_n(x)$ is irreducible over $\mathbf{Q}$.*

Solution. First, to see that the $\Phi_n(x)$ have integer coefficients, proceed by induction on n. The base case is $n = 1$, wherein $\Phi_1(x) = x - 1$ clearly has integer coefficients. Let $n > 1$ and assume that $\Phi_k(x)$ has integer coefficients for each $1 \leq k < n$ dividing n. Observe now that there is an identity

$$x^n - 1 = \prod_{k|n} \Phi_k(x)$$

where the product ranges over all integers k dividing n. In other words, $\Phi_n(x)$ may be expressed as the polynomial quotient of $x^n - 1$ by the product of the $\Phi_k(x)$ with k a proper divisor of n. The key point now is that there is a division algorithm for monic polynomials in $\mathbf{Z}[x]$: namely, given a monic polynomial $m(x) \in \mathbf{Z}[x]$ and *any* polynomial $f(x) \in \mathbf{Z}[x]$, then there are unique polynomials $g(x), r(x) \in \mathbf{Z}[x]$ such that

$$f(x) = m(x)g(x) + r(x)$$

where, furthermore, $\deg r(x) < \deg m(x)$. Applying this with

$$f(x) := x^n - 1 \text{ and } m(x) := \prod_{k|n, k \neq n} \Phi_k(x),$$

using that a product of monic polynomials is monic, shows that $g(x) = \Phi_n(x)$ has integer coefficients.

We prove that $\Phi_n(x)$ is irreducible using Galois theory. Choose a primitive n-th root of unity ζ. Then the n-th cyclotomic polynomial may be expressed as

$$\Phi_n(x) = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (x - \zeta^k)$$

where each power ζ^k is also a primitive n-th root of unity because k and n are coprime. Furthermore, since $\#(\mathbf{Z}/n\mathbf{Z})^\times = \phi(n)$, these are precisely all the primtive n-th roots of unity. This implies that the field extension $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ is the splitting field of $\Phi_n(x)$, whence Galois. On the one hand, the degree of this extension is at most $\deg \Phi_n(x) = \phi(n)$. On the other hand, each $k \in (\mathbf{Z}/n\mathbf{Z})^\times$ determines a unique $\mathbf{Q}$-automorphisms via $\zeta \mapsto \zeta^k$, yielding $\phi(n)$ distinct elements of $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$. This gives a matching lower bound the degree, showing that $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \phi(n)$ and that

$$\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times.$$

Since the action of the Galois group is transitive on the roots of $\Phi_n(x)$, this implies, as was seen on a previous set, that $\Phi_n(x)$ is irreducible. ∎

Problem 2. — *Let n be any positive integer and let $\mathbf{Q}_n := \mathrm{SF}_{\mathbf{Q}}(x^n - 1)$.*

(i) *Prove that $[\mathbf{Q}_n : \mathbf{Q}] = \phi(n)$ and $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$.*

(ii) *If m is an odd (positive) integer, prove that $\mathbf{Q}_{2m} = \mathbf{Q}_m$.*

(iii) *Find n such that $\mathbf{Q}_n$ contains a subfield which is not a cyclotomic extension of $\mathbf{Q}$.*

(iv) *Find all intermediate fields between $\mathbf{Q}$ and $\mathbf{Q}_8$, and between $\mathbf{Q}$ and $\mathbf{Q}_{12}$.*

Date: November 6, 2025.

Solution. Roots of the polynomial $x^n - 1$ are precisely the n-th roots of unity; comparing with the definition of the cyclotomic polynomials, this implies that there is a factorization

$$x^n - 1 = \prod_{k|n} \Phi_k(x)$$

where k ranges over all positive divisor of n. Observe that if k is any proper divisor of n, then any primitive k-th root of unity may be expressed as the (n/k)-th power of some primitive n-th root of unity, and so

$$\mathbf{Q}_n = \mathrm{SF}_{\mathbf{Q}}(x^n - 1) = \mathrm{SF}_{\mathbf{Q}}(\Phi_k(x) : k \mid n) = \mathrm{SF}_{\mathbf{Q}}(\Phi_n(x)) = \mathbf{Q}(\zeta)$$

where ζ is any choice of primitive n-th root of unity. The statements that $[\mathbf{Q}_n : \mathbf{Q}] = \phi(n)$ and $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$ of (i) now follows from the discussion of Problem 1.

For (ii), observe that for m odd, if ζ is any m-th root of unity, then $-\zeta$ is a $2m$-th root of unity. Thus all the roots of $x^{2m} - 1$ already lie in $\mathbf{Q}_m$, so that $\mathbf{Q}_{2m} = \mathbf{Q}_m$.

For (iii), one strategy to find a field extension of $\mathbf{Q}$ which is not isomorphic to a cyclotomic extension would be to find one whose degree d cannot be expressed as a totient value $\phi(m)$ for any integer m. Properties of the totient function may be used to show that the only way that $\phi(m)$ can be odd is if it is 1; in particular, any cubic extension of $\mathbf{Q}$ cannot be a cyclotomic extension. The simplest example in which $\mathbf{Q} \subset \mathbf{Q}_n$ has an intermediate extension that is cubic occurs when $n = 7$, so that the extension is sextic and has group $(\mathbf{Z}/7\mathbf{Z})^\times \cong C_6$. Let ζ be a primitive 7-th root of unity, so that $\mathbf{Q}_7 = \mathbf{Q}(\zeta)$. The intermediate extension $\mathbf{Q} \subset K \subset \mathbf{Q}(\zeta)$ is the fixed field of the order 2 subgroup determined by $\zeta \mapsto \zeta^{-1}$, that is $K = \mathbf{Q}(\zeta + \zeta^{-1})$.

For (iv), to find the intermediate fields of the two extensions $\mathbf{Q} \subset \mathbf{Q}_8$ and $\mathbf{Q} \subset \mathbf{Q}_{12}$, write their Galois groups as

$$\begin{aligned} \mathrm{Gal}(\mathbf{Q}_8/\mathbf{Q}) &\cong (\mathbf{Z}/8\mathbf{Z})^\times \cong C_2 \times C_2, \text{ and} \\ \mathrm{Gal}(\mathbf{Q}_{12}/\mathbf{Q}) &\cong (\mathbf{Z}/12\mathbf{Z})^\times \cong (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/4\mathbf{Z})^\times \cong C_2 \times C_2 \end{aligned}$$

where the final isomorphism on each line may be quickly verified by checking that every non-identity element has order 2. In both cases, there are three subgroups of order 2 which, by Galois theory, correspond to quadratic extensions of $\mathbf{Q}$. Handle each case in turn:

For $\mathbf{Q}_8$, these subgroups are generated by the residue classes of 3, 5, and 7. Write $\mathbf{Q}_8 = \mathbf{Q}(\zeta_8)$ where $\zeta_8 := e^{2\pi i/8}$. Since $\zeta_8^4 = -1$, we may compute the action of the Galois group elements on a general member of $\mathbf{Q}(\zeta_8)$ directly to see that

$$\begin{aligned} [3] \cdot (a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3) &= a + d\zeta_8 - c\zeta_8^2 + b\zeta_8^3, \\ [5] \cdot (a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3) &= a - b\zeta_8 + c\zeta_8^2 - d\zeta_8^3, \text{ and} \\ [7] \cdot (a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3) &= a - d\zeta_8 - c\zeta_8^2 - b\zeta_8^3. \end{aligned}$$

The corresponding fixed fields are therefore

$$\begin{aligned} \mathbf{Q}(\zeta_8 + \zeta_8^3) = \mathbf{Q}(\zeta_8 - \zeta_8^{-1}) &= \mathbf{Q}(\cos(2\pi/8)), \\ \mathbf{Q}(\zeta_8^2) &= \mathbf{Q}(i), \text{ and} \\ \mathbf{Q}(\zeta_8 - \zeta_8^3) = \mathbf{Q}(\zeta_8 + \zeta_8^{-1}) &= \mathbf{Q}(i\sin(2\pi/8)). \end{aligned}$$

For $\mathbf{Q}_{12}$, the subgroups are generated by the residue classes of 5, 7, and 11. Write $\mathbf{Q}_{12} = \mathbf{Q}(\zeta_{12})$ for $\zeta_{12} := e^{2\pi i/12}$. This time, it is easy to directly compute $\zeta_{12}^6 = -1$, but it is unclear how to express ζ_{12}^4 in terms of the $\mathbf{Q}$-basis of $\mathbf{Q}(\zeta_{12})$ given by 1, ζ_{12}, ζ_{12}^2, and ζ_{12}^3. For this, we need to determine the cyclotomic polynomial $\Phi_{12}(x)$. One way to compute this is to note that

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) = (x^6 - 1)\Phi_4(x)\Phi_{12}(x)$$

where the second equality comes from grouping the $\Phi_k(x)$ with k a divisor of 6. The remaining cyclotomic polynomial $\Phi_4(x)$ is easy to determine; $\Phi_1(x) = x-1$ and $\Phi_2(x) = x+1$, so that

$$\Phi_4(x) = (x^2-1)(x-1)^{-1}(x+1)^{-1} = x^2+1.$$

Thus

$$\Phi_{12}(x) = (x^{12}-1)(x^6-1)^{-1}(x^2+1)^{-1} = x^4-x^2+1.$$

This implies that $\zeta_{12}^4 = \zeta_{12}^2 - 1$, with which we may now compute the Galois group action on a general member of $\mathbf{Q}(\zeta_{12})$:

$$\begin{aligned}
[5]\cdot(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3) &= (a+c)-b\zeta_{12}-c\zeta_{12}^2+(b+d)\zeta_{12}^3,\\
[7]\cdot(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3) &= a-b\zeta_{12}+c\zeta_{12}^2-d\zeta_{12}^3, \text{ and}\\
[11]\cdot(a+b\zeta_{12}+c\zeta_{12}^2+d\zeta_{12}^3) &= (a+c)+b\zeta_{12}-c\zeta_{12}^2-(b+d)\zeta_{12}^3.
\end{aligned}$$

The fixed fields are determined in each case by the equations $b=c=0$, $b=d=0$, and $c=b+2d=0$, respectively. That is to say, the fixed fields are

$$\begin{aligned}
\mathbf{Q}(\zeta_{12}^3) &= \mathbf{Q}(i),\\
\mathbf{Q}(\zeta_{12}^2) &= \mathbf{Q}(\zeta_6), \text{and}\\
\mathbf{Q}(\zeta_{12}^3-2\zeta_{12}) &= \mathbf{Q}(\zeta_{12}+\zeta_{12}^{-1} = \mathbf{Q}(\cos(2\pi i/12)),
\end{aligned}$$

where the last one uses the identity $\zeta_{12}^3-2\zeta_{12} = (\zeta_{12}^4-2\zeta_{12}^2)\zeta_{12}^{-1} = -(\zeta_{12}+\zeta_{12}^{-1})$. ■

Problem 3. — *Prove that* $\mathbf{Q}(\cos(2\pi/n))/\mathbf{Q}$ *is a Galois extension for every* $n \in \mathbf{N}$.

Solution. Since $\zeta_n := e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$, we see that

$$2\cos(2\pi/n) = \zeta_n + \zeta_n^{-1}$$

and so $\mathbf{Q}(\cos(2\pi/n))$ is an intermediate field extension of the cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_n)$; in fact, this is the fixed field corresponding the order 2 subgroup generated by $\zeta_n \mapsto \zeta_n^{n-1} = \zeta_n^{-1}$. Since

$$\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$$

is abelian, the order 2 subgroup is normal, and so the main theorem of Galois theory implies that $\mathbf{Q} \subset \mathbf{Q}(\zeta_n+\zeta_n^{-1}) = \mathbf{Q}(\cos(2\pi/n))$ is a Galois extension of degree $\phi(n)/2$. ■

Problem 4. — *Consider a tower of field extensions* $K = K_0 \subset K_1 \subset \ldots \subset K_n = L$ *where each* K_{j+1}/K_j *is obtained by extracting an* m_j*-th root, where each* m_j *is invertible in* K*. Let* $m = \prod_{j=1}^n m_j$ *and consider the field* $F = K(\mu_m)$*. Prove that the tower of composite fields*

$$K \subset F = FK_0 \subset FK_1 \subset \ldots \subset FK_n = FL$$

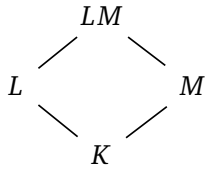
is a radical tower and that each FK_{j+1}/FK_j *is Galois with cyclic Galois group.*

Proof. Each FK_{j+1}/FK_j is obtained by adjoining the same m_j-th root, so the main thing to observe is that the extension $K \subset F$ is also radical, as the primitive m-th root μ_m is, well, a root of 1. That each FK_{j+1}/FK_j is Galois with cyclic Galois group now follows from the structure of cyclic field extensions over cyclotomic fields, the point being that F—and hence FK_j—has a primitive m_j-th root of unity by taking powers of μ_m. ■

Problem 5. — *Let* L/K *and* M/K *be two finite* Galois[1] *extensions such that* $L, M \subset \bar{K}$ *and* M/K *and* LM/M *are solvable. Prove that* L/K *is solvable as well.*

[1]The hypothesis is clarified here in the solutions. Without assuming that $K \subset L$ is Galois, the statement may become unclear, depending on what solvable extension is taken to mean: consider $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt[3]{2})$, and $M = \mathbf{Q}(\zeta_3)$, for example.

Proof. We have a diagram of field extensions



where each of the extensions in the tower $K \subset M \subset LM$ are solvable. In particular, that means that each extension therein is Galois and that there is a short exact sequence of Galois groups

$$1 \to \mathrm{Gal}(LM/M) \to \mathrm{Gal}(LM/K) \to \mathrm{Gal}(M/K) \to 1$$

where both the subgroup $\mathrm{Gal}(LM/M)$ and quotient group $\mathrm{Gal}(M/K)$ are solvable, whence so is $\mathrm{Gal}(LM/K)$. Galois theory now implies that $L \subset LM$ is a Galois extension; its Galois group is a subgroup of the solvable group $\mathrm{Gal}(LM/L)$, and so it is itself solvable; furthermore, since $K \subset L$ is Galois, this is a normal subgroup of $\mathrm{Gal}(LM/K)$ and fits in a short exact sequence

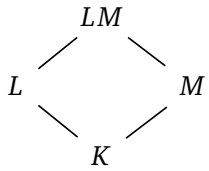
$$1 \to \mathrm{Gal}(LM/L) \to \mathrm{Gal}(LM/K) \to \mathrm{Gal}(L/K) \to 1.$$

Thus $\mathrm{Gal}(L/K)$ is a quotient of a solvable group, and so is also solvable. ∎

Problem 6. — *Let L/K and M/K be two finite Galois extensions. Prove that LM/M and $L/L \cap M$ are also Galois and that*

$$\mathrm{Gal}(LM/M) \simeq \mathrm{Gal}(L/L \cap M).$$

Proof. The intersection fits as an intermediate field extension $K \subset L \cap M \subset L$, so the main theorem of Galois theory shows that $L \cap M \subset L$ is also Galois; for the same reason, the extension $L \cap M \subset M$ is Galois, too. Replacing K by $L \cap M$ now only weakens the hypotheses present for the remaining statements, so without loss of generality, assume henceforth that $L \cap M = K$. In this setting, the two field extensions $K \subset L$ and $K \subset M$ are commonly referred to as *linearly disjoint* over K. The data in question now fits into a diagram of field extensions



where the bottom half consists of Galois extensions. We show that the top half also consists of Galois extensions: Write, for instance, $L = \mathrm{SF}_K(S)$ for a finite set of separable polynomials $S \subset K[x]$. Viewing S as a set of polynomials with coefficients in M then shows that $LM = \mathrm{SF}_M(S)$, whence LM is Galois over M. A symmetric argument shows that LM is Galois over L.

Regarding the Galois groups, observe that the assumption $L \cap M = K$ means that there is no nontrivial intermediate field extension of $K \subset LM$ lies in both L and M. This implies that there are no proper normal subgroups of $\mathrm{Gal}(LM/K)$ that contain both $\mathrm{Gal}(LM/L)$ and $\mathrm{Gal}(LM/M)$. Since the intersection of these two groups is the trivial subgroup $\{1\}$, this implies that

$$\mathrm{Gal}(LM/K) = \mathrm{Gal}(LM/L) \cdot \mathrm{Gal}(LM/M)$$

that is, each element of $\mathrm{Gal}(LM/K)$ may be uniquely written as a product of elements from the two groups on the left. Now consider the restriction map

$$\rho_L \colon \mathrm{Gal}(LM/K) \to \mathrm{Gal}(L/K).$$

Since $K \subset L \subset LM$ is a tower of Galois field extensions, this is surjective and its kernel is $\mathrm{Gal}(LM/L)$. That every element of $\mathrm{Gal}(LM/K)$ is uniquely written as an element of $\mathrm{Gal}(LM/L)$ and $\mathrm{Gal}(LM/M)$ now implies that the restriction of ρ_L to $\mathrm{Gal}(LM/M)$ is a isomorphism onto $\mathrm{Gal}(L/K)$. ■

Problem 7. — *Let L/K be a finite separable extension of prime degree p. Let $\alpha \in L$ be such that $L = K(\alpha)$ and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_p$ be the K-conjugates of α in $\bar{K}$. Prove that if $\alpha_2 \in L$, then L/K is Galois with cyclic Galois group.*

Solution. That the elements of $A := \{\alpha_1, \alpha_2, \ldots, \alpha_p\}$ are K-conjugate over $\bar{K}$ implies that for any finite Galois extension $K \subset M$ containing A, $\mathrm{Gal}(M/K)$ also acts transitively on A. Furthermore, the action gives a homomorphism $\mathrm{Gal}(M/K) \to S_p$ mapping the Galois group to a transitive subgroup of S_p. By the orbit-stabilizer theorem, this subgroup has order divisible by p, so by Cauchy's theorem it contains a p-cycle. In other words, there is an element $\sigma \in \mathrm{Gal}(M/K)$ with the property that, up to reindexing the α_i, $\sigma(\alpha_i) = \alpha_{i+1}$, where $\alpha_{p+1} =: \alpha_1$.

Consider now the subgroup $H \subset \mathrm{Gal}(M/K)$ that stabilizes α_1. The orbit-stabilizer theorem implies that this is an index $\#A = p$ subgroup. The corresponding intermediate field extension $K \subset M^H \subset M$ contains L and satisfies

$$[M^H : K] = \#\,\mathrm{Gal}(M/K)/\#H = p.$$

Multiplicativity of degrees for the tower $K \subset L \subset M^H$ thus shows that $L = M^H$. The hypothesis that $\alpha_2 \in L$ now implies that H also fixes α_2. But this implies that for any $h \in H$,

$$\sigma(h(\alpha_1)) = \sigma(\alpha_1) = \alpha_2 = h(\alpha_2) = h(\sigma(\alpha_1)).$$

Since α generates L over K, this implies that the restrictions of $\sigma \circ h$ and $h \circ \sigma$ to L coincide. Now a simple induction shows that $\alpha_i \in L$ for all i since, once we know $\alpha_{i-1} \in L = M^H$, then

$$h(\alpha_i) = h(\sigma(\alpha_{i-1})) = \sigma(h(\alpha_{i-1})) = \sigma(\alpha_{i-1}) = \alpha_i$$

meaning that α_i is fixed by H and thus lies in L. Finally, this implies that L is spanned over K by the members of A, from which it follows that the restriction $\sigma|_L$ is a well-defined element of $\mathrm{Aut}_K(L)$. Since this element has order p, this implies that $\#\,\mathrm{Aut}_K(L) \geq p = [L : K]$, and finally, this means that the extension $K \subset L$ is Galois with group a cyclic group of order p. ■