MATH 7211 Homework 7

Andrea Bourque

May 9, 2023

1 Problem 14.5.1

Determine the minimal polynomials satisfied by the primitive generators given in the text for the subfields of $\mathbb{Q}(\zeta_{13})$.

Proof. Let $\zeta = \zeta_{13}$. The generators in the text are $\zeta + \zeta^{12}, \zeta + \zeta^3 + \zeta^9, \zeta + \zeta^5 + \zeta^8 + \zeta^{12}, \zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12}$. The minimal polynomials of each generator is the polynomial with roots given by the generator and its distinct Galois conjugates, which are the expressions obtained by replacing ζ by ζ^k for $k = 1, ..., 12$. For instance, the minimal polynomial of the generator $\zeta + \zeta^{12}$ has roots $\zeta + \zeta^{12}, \zeta^2 + \zeta^{11}, \zeta^3 + \zeta^{10}, \zeta^4 + \zeta^9, \zeta^5 + \zeta^8, \zeta^6 + \zeta^7$. In particular, we must multiply out

$$(x - (\zeta + \zeta^{12}))(x - (\zeta^2 + \zeta^{11}))...(x - (\zeta^6 + \zeta^7)).$$

This is doable by hand, but I leave it to a computer (I used Singular CAS) to give this as $x^6 + x^5 - 5x^4 - 4x^3 + 6x^2 + 3x - 1$. The same method is used to determine the other minimal polynomials, in order of the generators as listed above: $x^4 + x^3 + 2x^2 - 4x + 3$, $x^3 + x^2 - 4x + 1$, $x^3 + x - 3$. $\square$

2 Problem 14.5.5

Let p be a prime and let $\epsilon_1, \epsilon_2, ...\epsilon_{p-1}$ denote the primitive pth roots of unity. Set $p_n = \epsilon_1^n + ... + \epsilon_{p-1}^n$. Prove that

$$p_n = \begin{cases} -1 & p \nmid n \\ p-1 & p \mid n \end{cases}.$$

Proof. If $p \mid n$, then $\epsilon_k^n = 1^{n/p} = 1$, so $p_n = 1 + ... + 1 = p - 1$. If $p \nmid n$, then n is invertible mod p, so multiplication by n is a bijection of the integers mod p. Without loss of generality, we can write $\epsilon_k = \exp(2\pi ik/p)$, and then $\epsilon_k^n = \exp(2\pi ink/p)$. By the bijection of the numbers $1, ..., p-1$ and $n, ..., n(p-1)$ mod p, we have that $p_n = p_1$. Finally, $p_1 = \zeta_p + ... + \zeta_p^{p-1} = -1 + \Phi_p(\zeta_p) = -1 + 0 = -1$, where $\Phi_p(x)$ is the cyclotomic polynomial $1 + x + ... + x^{p-1}$. □

3 Problem 14.5.10

Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Proof. Recall that the Galois group of a cyclotomic field over $\mathbb{Q}$ is abelian, so all of its subgroups are normal. Hence, by the fundamental theorem of Galois theory, any subextension of a cyclotomic field is Galois over $\mathbb{Q}$. But $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension, since it does not contain all the roots of the irreducible $x^3 - 2$, even though it contains at least one (i.e. it is not a normal extension). $\square$

4 Problem 14.5.11

Prove that the primitive nth roots of unity form a basis for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ iff n is squarefree.

Proof. Suppose n is not squarefree. Let p be a prime for which $p^2 \mid n$. Then $\zeta_n^{n/p}$ is a primitive pth root of unity, say ζ_p, and $1 + kn/p$ is coprime to n for $k = 1, ..., p-1$. Then $\zeta_n + \zeta_n^{1+n/p} + ... + \zeta_n^{1+(p-1)n/p} = \zeta_n(1 + \zeta_p + ... + \zeta_p^{p-1}) = \zeta_n \Phi_p(\zeta_p) = 0$. Thus if n is not squarefree, the primitive nth roots of unity are not linearly independent over $\mathbb{Q}$, so they cannot form a basis.

Next, we need some general machinery. Let K_1, K_2 be Galois extensions of a field F with $K_1 \cap K_2 = F$. Then Proposition 19 and Corollary 20 in Dummit and Foote Section 14.4 give that K_1K_2/F is Galois, and $[K_1K_2 : F] = [K_1 : F][K_2 : F]$. Let $\alpha_1, ...\alpha_m$ be a basis for K_1/F, and let $\beta_1, ..., \beta_n$ be a basis for K_2/F. By Proposition 21 in Dummit and Foote Section 13.2, $\{\alpha_i\beta_j\}$ spans K_1K_2 over F. Since There are mn elements of the form $\alpha_i\beta_j$, and they span the mn dimensional F vector space K_1K_2, they must be a basis for K_1K_2 over F.

We know that the primitive pth roots of unity $\zeta_p, ..., \zeta_p^{p-1}$ form a basis for the Galois extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, where p is prime. Let q be a prime distinct from p. From Corollary 27 in Dummit and Foote Section 14.5, we have that $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ and $\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_{pq})$. Then we can apply the remark in the previous paragraph to get that $\zeta_p^j\zeta_q^k$ for $j = 1, ..., p-1$ and $k = 1, ..., q-1$ is a basis for $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}$. By induction, for n square-free, we have a basis of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ consisting of products of primitive p_ith roots of unity for prime divisors p_i of n.

To finish the proof, we must show that these products of primitive p_ith roots of unity for prime divisors p_i of n are exactly the primitive nth roots of unity. Certainly they are nth roots of unity, since each p_ith root is an nth root, since $p_i|n$ so $\zeta_p^n = (\zeta_p^p)^{n/p} = 1$. They are primitive because any proper divisor $d > 1$ of n is also squarefree, hence a product of some p_i's, so raising the basis element to the dth power will eliminate the corresponding p_ith roots from the product, but will keep the p_jth roots for all p_j dividing n/d. Furthermore, since the products are a basis for the $\phi(n)$ dimensional $\mathbb{Q}$ vector space $\mathbb{Q}(\zeta_n)$, they are $\phi(n)$ of them. There are also $\phi(n)$ primitive nth roots of unity, so the basis must be exactly the primitive nth roots of unity as desired. □

5 Problem 14.6.18

Let θ be a root of $x^3 - 3x + 1$. Prove that the splitting field of this polynomial is $\mathbb{Q}(\theta)$ and that the Galois group is cyclic of order 3. Find the other roots of the polynomial written in the form $a + b\theta + c\theta^2$ for $a, b, c \in \theta$.

Proof. The discriminant of the cubic is $-4(-3)^3 - 27(1)^2 = 81$, which is a square in $\mathbb{Q}$. Thus the Galois permutations are even, so the Galois group is $\mathbb{Z}/3\mathbb{Z}$. In particular, $|\text{Gal}| = 3$, so the degree of the splitting field extension is also 3. Since $x^3 - 3x + 1$ is irreducible by the rational root theorem $(1 - 3 + 1 \neq 0, (-1)^3 - 3(-1) + 1 \neq 0)$, the extension $\mathbb{Q}(\theta)/\mathbb{Q}$ has degree 3 as well. Since the splitting field must contain $\mathbb{Q}(\theta)$, and the two extensions of $\mathbb{Q}$ have the same degree, they must be equal. Thus the splitting field is $\mathbb{Q}(\theta)$ as desired.

Now, let the other two roots be s, t. Say without loss of generality that $(\theta - s)(\theta - t)(s - t) = 9$ (the expression is either 9 or -9, up to choosing which root is s and which is t). We know from the given cubic that $\theta + s + t = 0, \theta s + \theta t + st = -3$. Then $s + t = -\theta, st = -3 - \theta(s + t) = \theta^2 - 3$. Then we have $(\theta^2 - (s + t)\theta + st)(s - t) = (3\theta^2 - 3)(s - t) = 9$. Then $s - t = \frac{3}{\theta^2 - 1}$. Let $(\theta^2 - 1)^{-1} = x + y\theta + z\theta$, so that

$$
\begin{aligned}
(\theta^2 - 1)(x + y\theta + z\theta^2) &= 1 \\
-x - y + (2y - z)\theta + (x + 2z)\theta^2 &= 1 \\
\begin{pmatrix} -1 & -1 & 0 \\ 0 & 2 & -1 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\
\begin{pmatrix} x \\ y \\ z \end{pmatrix} &= \begin{pmatrix} -4/3 \\ 1/3 \\ 2/3 \end{pmatrix}
\end{aligned}
$$

Thus $s - t = -4 + \theta + 2\theta^2$. Since $s + t = -\theta$, we have $s = -2 + \theta^2, t = 2 - \theta - \theta^2$. $\square$