Algebra 2 Homework 7

March 29, 2024

Solution of problem 1: Let ζ_n denote a primitive nth root of unity. Then see that -1 is a primitive 2nd root of unity. Also see that $-\zeta_n$ cannot have order n, since it is odd, so $-1^n = -1$. Thus, its order must be more than n. However, $(-\zeta_n)^{2n} = 1$, so its order must divide $2n$. The only such number is $2n$. Since the nth cyclotomic extension contains these elements, it must contain the $2n$th roots of unity. $\square$

Solution of problem 2: Since $A^k = I$ for some $k \geq 1$, the minimal polynomial $m(x)$ of A divides $x^k - 1$. Clearly, $x^k - 1$ is a polynomial with all distinct roots. The minimal polynomial has no repeated roots, hence it must be diagonalisable.

For $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, see that $A^k = \begin{pmatrix} 1 & k\alpha \\ 0 & 1 \end{pmatrix}$, for any $k \in \mathbb{N}$. This can easily be checked by induction. See that for $k = p$, we must have I since the field has characteristic p. See that the characteristic of A is just $x^2 - 1 = 0$, which gives us ± 1 as the eigenvalues. We see that the $\ker \dim(A - I) = \{(x, y) \in \mathbb{R}^2 \mid A - I(x, y)^T = 0\} = \dim(\text{ span } (1, 0)) = 1$, while $\ker \dim(A + I) = \{(x, y) \in \mathbb{R}^2 \mid A + I(x, y)^T = 0\} = \dim(\text{ span } (0, 0)) = 0$, which clearly does not add up to 2, since 1 and 2 are not the same number. Thus for $\alpha \neq 0$, this matrix is not diagonalisable. If $\alpha = 0$, in the eigenvalue -1, we would have the null space as $\text{ span } (0, 1)$, which would give us a basis for $\mathbb{R}^2$. $\square$

Solution of problem 3: We will make some mention of notation explictly detailing the structure of the Galois group of $K = \mathbb{Q}(\theta, i)$, where $\theta = \sqrt[8]{2}$. Let $\zeta = \frac{1}{2}\sqrt{2}(1 + i)$, a primitive 8th root of unity. This is a group of order 16 over $\mathbb{Q}$. Let $\sigma, \tau \in \text{Aut}(K/\mathbb{Q})$, where σ sends θ to $\zeta\theta$, i to i, and ζ to ζ^5. The last follows from the first two. Define τ such that it sends θ to θ, i to $-i$ and ζ to ζ^7. We can then see that $\sigma^8 = \tau^2 = e$, the identity automorphism. Also see that $\sigma\tau == \tau\sigma^3$, which can be checked by brute force. This completely characterises the Galois Group.

Now see that by the fundamental theorem of Galois theory, the subgroups corresponding to F_1, F_2, and F_3 are $\langle \sigma \rangle, \langle \sigma^2, \tau \rangle$, and $\langle \sigma^2, \tau\sigma^3 \rangle$.

Since F_1 is the fixed field of $\langle \sigma \rangle$, we have $K^{F_1} \cong \mathbb{Z}_8$. In the second case, the fixed field corresponds to the subgroup $\langle \sigma^2, \tau \rangle$. We have $(\sigma^2)^4 = \tau^2 = e$, and $\sigma^2\tau = \tau\sigma^{-2}$, which is the presentation for D_8. The subgroup corresponding to F_3 is $\langle \sigma^2, \tau\sigma^3 \rangle$. See that there is more than one element of order 4 in the group. The only such group is Q_8. $\square$

Solution of problem 4: We can see that $x^4 - 14x^2 + 0 = 0$ is solved as a quadratic in x^2, that is, $x^2 = 7 \pm 2\sqrt{10}$. We can write $7 - 2\sqrt{10} = 7 - 2\sqrt{10}\frac{7+2\sqrt{10}}{7+2\sqrt{10}} = \frac{9}{7+2\sqrt{10}}$. Then we can see that $x = \pm\sqrt{7 + 2\sqrt{10}}, \pm\frac{3}{\sqrt{7+2\sqrt{10}}}$. All of these roots lie in $K = \mathbb{Q}(\sqrt{7 + 2\sqrt{10}})$.

We propose that this field is Galois. The minimal polynomial for $\sqrt{7+2\sqrt{10}}$ is all in K, thus it is normal, since it contains all of its conjugates. It is also clear that none of the roots are repeated, so the extension is separable. Thus K is the Galois splitting field. $\square$

Solution of problem 5:

1. $[K : F] = n < \infty$, then we say that K is represented as by a finite $F-$basis, by $\{b_1, \ldots, b_n\}$. Let $x \in K$, where $x = \sum_{i=1}^{n} c_i b_i$, where $c_i \in F$ for $i = 1, \ldots, n$. Now we have $\alpha \cdot x = \sum_{i=1}^{n} c_i(\alpha \cdot b_i)$. Since $\alpha \cdot b_i \in K$, $\alpha \cdot b_i = \sum_{j=1}^{n} a_{ji} b_j$. Then we can put this in matrix form, by $T_\alpha := (a_{ji})$. By this, it is clear that T_α is a linear transformation, since it can be written as a matrix.
2. See that $m(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is the minimal polynomial of α, and $f(x)$ is the minimal polynomial of T_α. We know that T_α is a root of $m(x)$, and since $m(x)|f(x)$, since $f(x)$ also has T_α as a zero, and $f(x)$ is irreducible, then they must be equal.
3. See that the multiplication operator has a minimal polynomial $m(x)$, and characteristic polynomial $c(x)$. They must have the same roots, and since $m(x)$ is irreducible, we must have $c(x) = m(x)^{n/d}$, comparing the degrees. Then comparing terms, we have $Tr(\alpha) = \frac{-n}{d} a_{d-1} = -b_{n-1} = Tr(T_\alpha)$, and $N(\alpha) = (-1)^n a_{d-1}^{n/d} = (-1)^n b_0 = \det T_\alpha$.

$\square$

Solution of problem 6: We have proven in the previous assignment that $f(x) = x^p - x - a$ is irreducible over $\mathbb{F}_p$, and that it is separable. We know that if α is a root, then so is $\alpha + 1$. So it is easy to see that the automorphism $\sigma : x \mapsto x + 1$ is an automorphism. Clearly, $\sigma^p = e$. Since these are p such automorphisms σ^i, for $0 \leq i \leq p-1$, then the Galois group must be cyclic. $\square$

Solution of problem 7: In $E = \mathbb{Q}(\sqrt{1+\sqrt{2}})$,let $x = \sqrt{1+\sqrt{2}}$. Then $x(x^2-1)^2 = 2$. We get that $x^4 - 2x^2 - 1 = 0$. We can explicitly see that none of its roots are rational, so the polynomial we have must be the minimal polynomial. We can calculate the conjugates, which are

$$\pm\sqrt{1+\sqrt{2}}, \pm i\frac{1}{\sqrt{1+\sqrt{2}}}.$$

So it is easy to see that i is missing. Thus, by adjoining i, we can have a normal and separable extension containing $\sqrt{1+\sqrt{2}}$. We propose that $K = \mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$ is the Galois extension. We know K contains all the conjugates, so the Galois field must be sandwiched between K and F. But since $[K : F] = 2$, which is prime, we must have that either the field is equal to E or F, and it cannot be F, since the imaginary conjugates are not in F, the Galois closure must be E. $\square$

Solution of problem 8: If $p \mid n$, then $\sum_{i=1}^{p-1} \epsilon_i^n = \sum_{i=1}^{p-1} 1 = p - 1$. Else, let $\epsilon_j = e^{2\pi i j/p}$ for $1 \leq i \leq n-1$, then we have

$$\sum_{i=1}^{p-1} \epsilon_i^n = \sum_{i=1}^{p-1} \epsilon_i^{ni} = \frac{\epsilon_i^{np} - \epsilon_i^n}{\epsilon_i^n - 1} = -1.$$

$\square$

Solution of problem 9*:* If $\mathbb{Q}(\zeta_n)$ contained $\mathbb{Q}(\sqrt[3]{2})$, then it must also contains its Galois closure, $\mathbb{Q}(\sqrt[3]{2}, \omega)$. The Galois group of this field is S_3, a non-abelian group contained in $\mathbb{Q}(\zeta_n)$, which must have a abelian Galois group, which is impossible. $\square$