Algebra 2 Homework 8

April 9, 2024

Solution of problem 1*:* Since x^3+ax+b is irreducible, then the discriminant $\Delta = -4a^3-27b^3$ is a square if and only if the Galois group is A_3. The splitting field of F_{p^n} must be isomorphic to $F_{p^{3n}}$, since our polynomial is irreducible. Then since $[F_{p^{3n}} : F_{p^n}] = 3$, which is the order of the Galois group of the splitting field, we have that the Galois group is A_3, hence Δ is a square. $\square$

Solution of problem 2*:* The resolvent of the polynomial x^4+2x^2+x+3 is x^3-4x^2-8x-1. See that modulo 3 the polynomial $x^3 - x^2 + x - 1$ is irreducible, and thus it must be irreducible in $\mathbb{Q}$. The discriminant of this polynomial is 3877, which is not a square, thus the Galois group is S_4. $\square$

Solution of problem 3*:* If K has $x^4 + ax^2 + b$ as its minimal polynomial, then we can do some calculations to see that

$$K = \mathbb{Q}\left[\sqrt{\frac{-a+\sqrt{a^2-4b}}{2}}, \sqrt{\frac{-a-\sqrt{a^2-4b}}{2}}\right].$$

(If $a^2 - 4b$ is not a square, and the two elements adjoined to $\mathbb{Q}$ aren't squares, then we can do the next steps). We can then see that $\sqrt{a^2-4b} \in K$, since if $\alpha = \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}}$, then $\sqrt{a^2-4b} = 2\alpha^2 + a \in K$. Clearly, $\mathbb{Q}(\sqrt{a^2-4b})$ is a quadratic extension that will lie in K.

Let F contain $\mathbb{Q}(\sqrt{\alpha})$, a field of degree 2. Then we must have that F is a quadratic extension of this field, hence we must have $F = \mathbb{Q}(\sqrt{a+\sqrt{\alpha}})$. It can now be seen that the minimal polynomial for $\sqrt{a+\sqrt{\alpha}}$ must be a biquadratic polynomial. $\square$

Solution of problem 4*:*

1. The automorphisms of $\mathrm{Gal}(K/F)$ are cyclic of order n. Let σ be an automorphism .Then we only need to see where σ sends $\sqrt[n]{a}$. Clearly $\sigma(\sqrt[n]{a}) = (\zeta_n)^i \sqrt[n]{a}$, where ζ_n is a primitive nth root of unity, and $i \in \mathbb{Z}$. Since $\sigma^d = i$, ζ_n^i is a dth root of unity.
2. See that $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ and $\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$ both are primitive dth roots of unity. Then we must have that the two are such that $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \left(\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^i$, for some i coprime to d. See that $\sigma\left(\frac{\sqrt[n]{a}}{\sqrt[n]{b}^i}\right) = \frac{\sqrt[n]{a}}{\sqrt[n]{b}^i}$, which means that this element lies in the fixed field of the automorphism, which is F. Thus it lies in F.

3. If $K = F(\sqrt[n]{a}) = F(\sqrt[n]{b})$, then by the previous problem we have $a = b^i \left(\frac{\sqrt[n]{a}}{\sqrt[n]{b}^i}\right)^n$, and a similar expression for b. The term in the brackets is in F, which is the required result. $\square$

Solution of problem 5*:* By Cauchy's theorem, G has a subgroup H of order p, which gives us a subfield F of L such that $[L : F] = p$. If we say that for all $\sigma \in G$ we have $\sigma(\alpha) \in F$, then we would have $F = L$. This is not possible, hence there is some $\sigma \in G$ where $\sigma(\alpha) \notin F$. Since P is prime and degree multiplies then $F(\sigma(\alpha)) = L$. See that $F' = \sigma^{-1}(F)$ is our required field. $\square$

Solution of problem 6*:* Any Galois extension of F in $K = F(\sqrt[n]{a})$ is trivial if n is odd and if n is even then the only non-trivial Galois extension. In either case, $[K : F] \leq 2$. $\square$

Solution of problem 7*:* We know that S_p is generated by a $p-$cycle and a transposition. To show this, see that we just need to check that any transposition can be generated using these two. Without loss of generality, assume that the two permutations are $(1, 2)$ and $(1, 2, \ldots, p)$. Now see that $(m, k) = (1, m)(1, k)(1, m)$, and $(1, k+1) = (1, k)(k, k+1)(1, k)$. Thus if we could generate $(k, k+1)$ for all k then we are done since we could generate $(1, k)$ inductively. Now see that $(k, k+1) = (1, 2, \ldots, p)(k-1, k)(1, 2, \ldots, p)^{-1}$, so inductively using $(1, 2)$ we can generate the entire group S_p.

We want to show that a polynomial with exactly 2 non-real roots has its Galois group as S_p. Let E be the splitting field of f in $\mathbb{C}$, and let $\alpha \in E$ be a root of f. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, so $p \mid [E : \mathbb{Q}]$. Thus the Galois group must contain an element of order p by Cauchy's theorem, which gives us p cycles in S_p. If we consider σ, complex conjugation, then it must flip the two non-real roots, and fix the others. Then that gives us an element of order 2 in the Galois group, which generates S_p.

Now pick a polynomial $f(x) = (x^2 + m)(x - n_1)\ldots(x - n_{p-2})$, where $m > 0$, and $n_i = n_j \implies i = j$, all even. Consider the polynomial $g(x) = f(x) - 2/n$, where n is such that $2/n < \varepsilon$, where $\varepsilon = \min_{f'(x)=0} = |f(x)| > 0$. This must also have $p - 2$ roots, and 2 non-real roots. Now see that $ng(x)$ fulfills Eisenstein's criterion since all coefficients of x^i for $i < p$ are even, and the constant term does not divide 4. This must have S_p as its Galois group. $\square$