SOLUTION SET 10

Problem 1 *Let α be a complex number. We define α to be an algebraic integer if it obeys a polynomial relation of the form $\alpha^n + c_1\alpha^{n-1} + \cdots + c_{n-1}\alpha + c_n = 0$ with the c_i integers.*

(a) Show that α is an algebraic integer if and only if the $\mathbb{Z}$ module spanned by 1, α, α^2, α^3, ... is finitely generated over $\mathbb{Z}$.

Suppose that α is an algebraic integer. We show, by induction on m, that α^m is in the $\mathbb{Z}$-span of 1, α, ..., α^{n-1}. This shows that the $\mathbb{Z}$-module spanned by 1, α, α^2, α^3, ... is generated by 1, α, ..., α^{n-1}. For $m \leq n-1$, the claim is trivial. For m larger, we have

$$\alpha^m = c_1\alpha^{m-1} + \cdots + c_{n-1}\alpha^{m-n+1} + c_n\alpha^{m-n}.$$

Inductively, all the terms on the left hand side are in the $\mathbb{Z}$-span of 1, α, ..., α^{n-1}, so α^m is as well.

In the reverse direction, let L_i be the $\mathbb{Z}$-span of 1, α, α^2, ..., α^i and let $L_\infty = \bigcup L_i$. Suppose that L_∞ is finitely generated over $\mathbb{Z}$, with generators e_1, e_2, ..., e_s. Then each e_j is in some L_i. By taking n large enough, we can arrange that e_1, e_2, ..., e_s are all in L_{n-1}, so $L_{n-1} = L_\infty$.. Then $\alpha^n \in L_n = L_\infty = L_n$, and we deduce that

$$\alpha^n = c_1\alpha^{n-1} + \cdots + c_{n-1}\alpha + c_n$$

for some integers c_i.

(b) Show that, if α and β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$.

Suppose that α obeys a monic polynomial of degree m and β obeys a monic polynomial of degree n. Then the $\mathbb{Z}$-span of the powers of $\alpha+\beta$, and also of the powers of $\alpha\beta$, is contained in the $\mathbb{Z}$-span of $\alpha^i\beta^j$ with $0 \leq i < m$ and $0 \leq j < n$.

(c) Show that, if α is an algebraic integer, then the minimal polynomial of α over $\mathbb{Q}$ is of the form $\alpha^n + c_1\alpha^{n-1} + \cdots + c_{n-1}\alpha + c_n = 0$ with the c_i integers. (Hint: Quote something from a previous problem set.)

Suppose that $d(\alpha) = 0$, where $d(x)$ is a polynomial with integer coefficients and leading coefficient 1. Let $c(x)$ be the minimal polynomial of α, normalized to also have leading coefficient 1. Then $d(x) = b(x)c(x)$ for some polynomial $b(x) \in \mathbb{Q}[x]$, which also has leading coefficient 1.

By Problem Set 8, problem CITE, there is a rational number r such that $rb(x)$ and $r^{-1}c(x)$ have integer coefficients. Looking at leading terms, both r and r^{-1} are integers. So $r = \pm 1$, and the coefficients of $c(x)$ are integers, as desired.

Problem 2 *Let $f(x)$ be an irreducible polynomial of degree 4 with rational coefficients and roots α_1, α_2, α_3 and α_4. Suppose that α_1 and α_2 are real and α_3 and α_4 are not real.*

(a) Let

$$\beta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4).$$

Show that β^2 is a negative rational number.

This was the problem from a QR exam. Any permutation of the α's takes β to $\pm\beta$, and hence fixes β^2. So β^2 is fixed by the Galois group, and is hence a rational number.

Let σ be complex conjugation, so $\sigma(\alpha_1) = \alpha_1$, $\sigma(\alpha_2) = \alpha_2$, $\sigma(\alpha_3) = \alpha_4$ and $\sigma(\alpha_4) = \alpha_3$. We compute that $\sigma(\beta) = -\beta$, so β is a purely imaginary number, and β^2 is negative.

(b) Show that the Galois group of the splitting field of f over $\mathbb{Q}$ is either S_4 or $D_{2\cdot 4}$.

Let G be the Galois group. We will consider G as a subgroup of S_4.

G contains the element σ which interchanges 3 and 4. It also must act transitively on the $\{1,2,3,4\}$'s, since f is irreducible. Let τ be a permutation which takes 3 to 2.

If $\tau(4) = 4$ or 3, then σ and $\tau\sigma\tau^{-1}$ together generate all permutations of 234. So the stabilizer of 1 under the G-action has size 6 in this case and the group of S_4.

If $\tau(4) = 1$, then G contains (12) and (34). If τ is (32)(41), then τ, (12) and (34) generate a copy of $D_{2\cdot 4}$. So, in that case G contains the 8 element group $D_{2\cdot 4}$, and must have order either 8 or 24. If τ is (41), then (12), τ and (34) already generate all of S_4.

Problem 3 *Inside the group S_5, let $\sigma = (1243)$ and let $\tau = (12345)$. Let T be the subgroup of S_5 generated by τ, and let D be the subgroup generated by σ and τ.*

(a) Check that T is normal in D, and $|D| = 20$.

We have $\sigma\tau\sigma^{-1} = \tau^2$, so $\sigma T \sigma^{-1} = T$. We also obviously have $\tau T \tau^{-1} = T$. Since D is generated by σ and τ, the subgroup T is normal in D.

Since σ and τ generate G, and $\tau \in T$, we see that σ generates D/T. Since σ, σ^2 and σ^3 are not in T, we have that $D/T \cong \mathbb{Z}/4$, so $|D| = 20$.

Let k be a field of characteristic zero containing primitive 4th and 5th roots of unity, call them i and ζ. Let $L = k(\theta_1, \theta_2, \ldots, \theta_5)$, the field of rational functions in 5 independent variables θ_1, θ_2, $\ldots$, θ_5; let S_5 act on L by permuting the θ's. Let $K \subset F \subset F' \subset L$ be the fixed fields of S_5, D, T respectively.

(b) What are the degrees of the extensions F/K, F'/F and L/F'?

The degrees of F/K, F'/F and L/F' are 6, 4 and 5, respectively.

Set $\alpha = \sum_{j=1}^5 \theta_j \zeta^j$.

(c) Show that $\alpha^5 \in F'$ and $L = F'(\alpha)$.

Observe that $\tau(\alpha) = \zeta\alpha$. So $\tau(\alpha^5) = \zeta^5\alpha^5 = \alpha^5$ and α^5 is fixed by τ. Since L/F' is of order 5, the field L is generated by any element not in F', and the element α is clearly not in F'.

(d) Find an element $\beta \in F'$ so that $\beta^4 \in F$ and $F' = F(\beta^4)$.

There are many options, but my favorite is the following. Let $\delta_1 = \alpha^5$. Let $\delta_2 = \sigma(\alpha^5) = \left(\sum_{j=1}^5 \theta_{2j}\zeta^j\right)^5$ (where indices are modulo 5) and define δ_3 and δ_4 analogously. Set

$$\beta = \delta_1 + \delta_2 i + \delta_3(-1) + \delta_4(-i).$$

Then $\sigma(\beta) = i\beta$. So $\sigma(\beta^4) = \beta^4$ and $\beta^4 \in F$.

In order to show that $F(\beta) = F'$, we just must show that β is not in F, nor in the quadratic extension of F. Since $\sigma^2(\beta) = -\beta$, the element β is not fixed by σ^2 and we are done.

(e) Let $\gamma = \beta^4$ be the element that you found in the previous problem. Show that γ obeys a polynomial of degree 6 over K.

Since γ is in F, it is fixed by D. So γ has $6 = \#(S_5)/\#(D)$ conjugates under the action of S_5. The polynomial $\prod_{g \in S_5/D}(x - g(\gamma))$ has coefficients in K, by symmetry, and degree 6.

This polynomial was explicitly computed by Lagrange, and is known as the Lagrange resolvent.

Problem 4 *Let ζ be a primitive n-th root of unity. The aim of this problem is to show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is all of $(\mathbb{Z}/n)^*$ (we have already shown that it is a subgroup of $(\mathbb{Z}/n)^*$).*

Define $\phi(x) = \prod_{a \in \mathbb{Z}/n^*}(x - \zeta^a)$.

(a) Compute ϕ for $1 \leq n \leq 6$. The coefficients of ϕ should be integers. (Feel free to use a computer algebra system.)

$$x - 1,\ x + 1,\ x^2 + x + 1,\ x^2 + 1,\ x^4 + x^3 + x^2 + x^2 + x + 1,\ x^2 - x + 1$$

(b) Prove that, for any n, the coefficients of ϕ are integers. (Hint: See problem 1, and feel free to use results from that problem which you haven't proved.)

An n-th root of unity is an algebraic integer, since it obeys $x^n - 1 = 0$. So the coefficients of ϕ are algebraic integers, since they are sums of products of algebraic integers. The coefficients of ϕ are also rational, since they are Galois invariant. So the coefficients of ϕ are integers.

(c) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta), \mathbb{Q})$ is $(\mathbb{Z}/n)^*$ if and only if $\phi(x)$ is irreducible.

If $\mathrm{Gal}(\mathbb{Q}(\zeta), \mathbb{Q})$ is all of $(\mathbb{Z}/n)^*$, then all of the roots of ϕ are in a single Galois orbit, so ϕ is irreducible. Conversely, if $\mathrm{Gal}(\mathbb{Q}(\zeta), \mathbb{Q})$ is all of $(\mathbb{Z}/n)^*$ is a proper subgroup H of $(\mathbb{Z}/n)^*$, then $\prod_{a \in H}(x - \zeta^a)$ will have integer coefficients and will divide $\phi(x)$.

(d) Let p be a prime not dividing n. Show that $x^n - 1$ is separable in $\mathbb{F}_p[x]$.

We just compute $GCD(x^n - 1, nx^{n-1}) = 1$.

Suppose for the sake of contradiction that $\phi(x) = f(x)g(x)$ with f irreducible.

(e) Show that the coefficients of f and g are integers.

This is the same argument as in 1(c): Normalize f and g to have leading coefficient 1. There is a rational number r such that both $rf(x)$ and $r^{-1}g(x)$ have rational coefficients. But looking at leading terms shows that r and r^{-1} are both integers, so $r = \pm 1$ and $f(x)$ and $g(x)$ have integer coefficients.

*(f) (**Harder**) Let p be a prime not dividing n. Suppose, for the sake of contradiction, that $f(\zeta) = 0$ and $f(\zeta^p) \neq 0$. Show that, in $\mathbb{F}_p[x]$, the polynomial $f(x)$ divides $g(x)$. (This question makes sense because the coefficients of f and g are integers.)*

Since ζ^p is a root of $\phi(x)$, and $f(\zeta^p)$ is assumed not to be zero, we must have $g(\zeta^p) = 0$. So ζ is a root of both $f(x)$ and $g(x^p)$. Since f is irreducible, this means that $f(x)$ divides $g(x^p)$: Say $f(x)h(x) = g(x^p)$. Reducing this relationship modulo p, we obtain $f(x)h(x) = g(x^p) = g(x)^p \mod p$. So f divides $g(x)^p$ in $\mathbb{F}_p[x]$. As $x^n - 1$ is separable modulo p, so are all it factors and f is separable modulo p. So $f(x)|g(x) \mod p$.

(g) Deduce that, for any prime p not dividing n, if $f(\zeta) = 0$ then $f(\zeta^p) = 0$.

We previously showed that, if $f(\zeta) = 0$ and $f(\zeta^p) \neq 0$, then $f(x)|g(x)$ modulo p. But then $f(x)^2$ divides $\phi(x)$ modulo p, contradicting that $\phi(x)$ is separable modulo p.

*(h) Show that, for any a relatively prime to n, $f(\zeta^a) = 0$. (You do **not** need to use Dirichlet's theorem that there is a prime p congruent to $a \mod n$.)*

Factor a into primes as $p_1 p_2 \cdots p_s$. Part (g) shows that, if ζ is a root of f then so is ζ^{p_1}. Applying the result again, $\zeta^{p_1 p_2}$ is also a root of f and so forth, up to $\zeta^{p_1 p_2 \cdots p_s} = \zeta^a$ being a root of f.