

MATH 121 SOLUTION SET 7

1. Suppose that $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of prime degree p and that $f(x)$ has exactly two roots that are not real. Prove that the Galois group of $f(x)$ over \mathbb{Q} is isomorphic to S_p .

Solution: We'll prove that the Galois group of $f(x)$ is isomorphic to a transitive subgroup of S_p which contains a 2-cycle. Then exercise 6 from the previous problem set tells us that G is isomorphic to S_p .

First of all, we know that G (G is the Galois group of $f(x)$) acts on the set of roots of $f(x)$ by permuting them. Since $f(x)$ is irreducible and since \mathbb{Q} has characteristic 0, we know that the roots are distinct and so we may view G as a subgroup of S_p (or, equivalently, G is isomorphic to a subgroup of S_p). We know that given any two distinct roots of $f(x)$, there exists an element in the Galois group of $f(x)$ that takes one of these roots to another one. Hence G is a transitive subgroup of S_p .

If L denotes a splitting field for $f(x)$ then we may view L as a subfield of \mathbb{C} . We know that the complex conjugation is an automorphism of \mathbb{C} and since L is a Galois extension over \mathbb{Q} , the restriction of the complex conjugation to L gives us an automorphism of L , i.e. an element of G . This automorphism fixes all real roots of $f(x)$ and interchanges the complex ones. Hence this element of G corresponds to a 2-cycle (viewing G as a subgroup of S_p). Therefore G is isomorphic to a transitive subgroup of S_p which contains a 2-cycle. Hence G is isomorphic to S_p .

2. Let $f(x)$ be a polynomial of degree n with integer coefficients. (a) Prove that for every $\epsilon > 0$, there is an irreducible polynomial $g(x) \in \mathbb{Q}[x]$ of degree n each of whose coefficients is within ϵ of the corresponding coefficient of $f(x)$.

Solution: Part a) follows immediately from part b), but here we'll give a proof that does not depend on part b). Let's write $f(x) = a_0 + a_1x + \cdots + a_kx^k$. Choose a prime number p such that $(1/p) < \epsilon$; this can be done since there are infinitely many primes. Define $g(x) = (a_0 + (1/p)) + (a_1 + (1/p))x + \cdots + (a_{k-1} + (1/p))x^{k-1} + (a_k + (1/p^2))x^k$. I claim that $g(x)$ is irreducible over \mathbb{Q} . Indeed, note that $p^2g(x) = (p^2a_0 + p) + (p^2a_1 + p)x + \cdots + (p^2a_{k-1} + p)x^{k-1} + (p^2a_k + 1)x^k$. Note that all the coefficients except for the leading one are divisible by p and that the constant coefficient is not divisible by p^2 . Hence $p^2g(x)$ is irreducible over \mathbb{Q} by Eisenstein's criterion. But p^2 is a unit in \mathbb{Q} and hence we conclude that $g(x)$ is irreducible over \mathbb{Q} , as desired.

b) Prove that it suffices to change the constant term. In other words, prove that there is a $q \in \mathbb{Q}$ with $|q| < \epsilon$ such that $f(x) + q$ is irreducible.

Solution: We showed on problem set 1 that if $p(x) = b_0 + b_1x + \dots + b_sx^s \in F[x]$ has degree n and if $x^n p(1/x)$ is irreducible over F then so is $p(x)$. In particular, if $x^n p(1/x)$ satisfies Eisenstein's criterion then we may conclude that $p(x)$ is irreducible. Now, to say that $x^n p(1/x)$ satisfies Eisenstein's criterion is to say that b_1, \dots, b_s are divisible by some prime q , that b_s is not divisible by q^2 and that q does not divide b_0 . Let's call this the reverse Eisenstein's criterion.

Let p be a prime such that $1/p < \epsilon$ and such that p doesn't divide a_k . Then let $q = 1/p$ so that $f(x) + q = (a_0 + (1/p)) + a_1x + \dots + a_kx^k$. Note that $p(f(x) + q) = (pa_0 + 1) + pa_1x + \dots + pa_kx^k$. Note that the constant coefficient is not divisible by p , that all other coefficients are divisible by p and that the leading coefficient is not divisible by p^2 . Hence $p(f(x) + q)$ satisfies the reverse Eisenstein's criterion and so it is irreducible. From this we conclude that $f(x) + q$ is irreducible over \mathbb{Q} too.

3(a). Find the Galois group of $x^4 + 4$ over \mathbb{Q} .

Solution: Note that this polynomial factors over \mathbb{Q} as $x^4 + 4 = x^4 + 4 + 4x^2 - 4x^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$. We see that its roots in \mathbb{C} are $\pm 1 \pm i$ and so its splitting field over \mathbb{Q} is $\mathbb{Q}(i)$. It has degree 2 over \mathbb{Q} and so the Galois group also has order 2. Hence the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

(b). Find the Galois group of $x^3 - x + 1$ over \mathbb{Q} .

Solution: This polynomial is irreducible over \mathbb{Q} (because it has no roots in \mathbb{Q}). Note that the discriminant of this polynomial is 81 which is a square in \mathbb{Q} . So we conclude that the Galois group is A_3 . (See the discussion of Galois groups of polynomials of degree 3 in the text, pp.611 - 613)

(c). Find the Galois group of $3x^3 - 3x + 1$ over \mathbb{Q} .

Solution: This polynomial is also irreducible over \mathbb{Q} because it has no roots in \mathbb{Q} . Computing the discriminant of this polynomial (or, more precisely, of $x^3 - x + (1/3)$) we get 1, which is a square in \mathbb{Q} . Hence the Galois group is again A_3 .

4. Suppose that L is a subfield of \mathbb{R} . Suppose also that $a \in \mathbb{R}$, $a^n \in L$, and that $a^k \notin L$ if $k < n$. Prove that $x^n - a^n$ is the minimal polynomial of a in $L[x]$.

Solution: Note that in \mathbb{C} the roots of $x^n - a^n$ are $a\zeta^i$ for $0 \leq i \leq n-1$; here ζ denotes the primitive n^{th} root of unity. So if $g(x)$ is the minimal polynomial for a over L then over \mathbb{C} it will factor as $(x - a\zeta^{k_1})(x - a\zeta^{k_2}) \dots (x - a\zeta^{k_r})$. Its constant coefficient is $a^r \zeta^j$ (for some integer j) and by assumption it lies in L . Since L is a subfield of \mathbb{R} , it follows that $|a^r \zeta^j|$ is also in L ; here $|\cdot|$ denotes the absolute value. But $|a^r \zeta^j| = \pm a^r$ and so we see that $a^r \in L$. From the given assumptions it follows that $r \geq n$, so the minimal polynomial of a over L must have degree at least n . But $x^n - a^n$ has degree n and a is one of its roots and hence we conclude that it is the minimal polynomial of a over L .

5. Let F be a subfield of \mathbb{R} . Let $f(x) \in F[x]$ be an irreducible polynomial of odd (!) degree such that all the roots of $f(x)$ are real. Let a be one of the roots of $f(x)$. (a). Suppose $F \subset L \subset L(r) \subset \mathbb{R}$ where L is a field and $r^p \in L$ for some odd prime number p . Show that if $a \in L(r)$, then $a \in L$.

Solution: We begin by observing if $r \in L$ then there's nothing to prove, so we may as well assume that $r \notin L$. Note that $r^d \notin L$ for any $d < p$. Indeed, if $r^d \in L$ for some $d < p$ then d and p must be coprime and so there exist integers a and b such that $ap + bd = 1$. But then $r = r^1 = r^{ap+bd} = (r^p)^a \cdot (r^d)^b$ and so $r \in L$. Hence the previous exercise tells us that $x^p - r^p$ is the minimal polynomial of r over L . Thus

$$[L(r) : L] = p.$$

We know that the other roots of $t^p - r^p$ are of the form $r\zeta^i$ for some i , $1 \leq i \leq p-1$. We know that there's an isomorphism from $L(r)$ to $L(r\zeta^i)$ which is the identity on L and it maps r to $r\zeta^i$; call this isomorphism ϕ . Now, we know that $\phi(a)$ is also a root of $f(x)$ so it is a real number. Hence $\phi(a) \in \mathbb{R} \cap L(r\zeta^i)$. Now $\mathbb{R} \cap L(r\zeta^i)$ is a subfield of $L(r\zeta^i)$ which contains L and since $L(r\zeta^i)$ has degree p over L , it follows that $\mathbb{R} \cap L(r\zeta^i) = L$ or $L(r\zeta^i)$. But since $\zeta^i \notin \mathbb{R}$ and since $r \in \mathbb{R}$, it follows that $\mathbb{R} \cap L(r\zeta^i) = L$. Hence $\phi(a) \in L$ and therefore $a \in L$ since ϕ is the identity on L .

Note: The result is not true for even p . For example, consider a cubic polynomial in $f(x) \in \mathbb{Q}[x]$ whose Galois group is S_3 and all of whose roots are real. Note that $[K : \mathbb{Q}] = 6$, where K is the splitting field. Let b be one of the roots. Then $[\mathbb{Q}(b) : \mathbb{Q}] = 3$. Thus $\mathbb{Q}(b)$ does not contain K , and therefore it does not contain all the roots of $f(x)$. That is, there is some root a of $f(x)$ such that $a \notin \mathbb{Q}(b)$. Now let $F = \mathbb{Q}$ and $L = \mathbb{Q}(b)$. Then

$$[K : L] = \frac{[K : \mathbb{Q}]}{[L : \mathbb{Q}]} = \frac{6}{3} = 2.$$

Thus K is a quadratic extension of L , so $K = L(r)$ for some r with $r^2 \in L$.

(b). Show that a is not contained in any real root extension of F . That is, there is no root extension E of F such that $a \in E \subset \mathbb{R}$.

Solution: See the remark after problem 4 in hw 8.