

MATH 121 SOLUTION SET 8

1. For each prime number p , prove that there is a degree p polynomial in $\mathbb{Q}[x]$ whose Galois group is isomorphic to S_p .

Solution: Let $f(x) = (x^2 + 1)(x - 1)(x - 2) \dots (x - (p - 2))$. Note that $f(x)$ has degree p and it has exactly $p - 2$ real roots. Of course, f is not irreducible, but we showed on the previous problem set that given any $\epsilon > 0$ we may find $q \in \mathbb{Q}$ such that $|q| < \epsilon$ and $f(x) + q$ is irreducible. We claim that if $\epsilon > 0$ is small enough, then $f(x) + q$ will have exactly $p - 2$ real roots. By hw7, problem 1, $f(x) + q$ will then have Galois group S_p as desired.

Thus it suffices to prove the claim:

Lemma 1. *Let $f(x) \in \mathbb{R}[x]$ be a monic polynomial with exactly k real zeroes, all simple. (There may be complex zeroes as well.) There is an $\epsilon > 0$ such that for all $c \in (-\epsilon, \epsilon)$, the polynomial $f(x) + c$ has exactly k real zeroes, all simple.*

Proof. Let $a_1 < a_2 < \dots < a_m$ be the real roots of $f'(x)$. Let ϵ be the minimum of $|f'(a_i)|$ for $1 \leq i \leq m$. Note that $\epsilon > 0$ since all the real roots of $f(x)$ are simple. Let $c \in \mathbb{R}$ with $|c| < \epsilon$. Then $f(x) + c$ and its derivative $f'(x)$ have no common zeroes, so all the real roots of $f(x) + c$ are simple.

Let $a_0 = -\infty$, $a_{m+1} = \infty$, $f(\infty) = \infty$, and let $f(-\infty)$ be ∞ or $-\infty$ according to whether the degree of $f(x)$ is even or odd. Note that for each i , $f(a_i)$ and $f(a_i) + c$ have the same sign (by choice of c).

For each $i = 1, \dots, m + 1$, the function $f(x)$ is strictly monotonic on the interval $a_{i-1} < x < a_i$ and therefore has at most one root in that interval. Furthermore, it has a root in that interval if and only if $f(a_{i-1})$ and $f(a_i)$ have opposite signs. Thus the number of real roots of $f(x)$ is equal to the number of i for which $f(a_i)$ and $f(a_{i-1})$ have opposite signs. Exactly the same reasoning applies to $f(x) + c$. It follows that (for $|c| < \epsilon$) $f(x)$ and $f(x) + c$ have the same number of real roots. \square

The lemma also follows readily from Rouché's Theorem (in complex analysis).

2. Consider the polynomial: $g(x) = x^5 + 2x^4 + 3x^3 + 4x + 5$. Find the sum of the reciprocals of the roots.

Solution: Let $\theta_1, \theta_2, \theta_3, \theta_4, \theta_5$ denote the roots of this polynomial (in \mathbb{C}). Then from the discussion on pp.607 - 608 of the text we know that elementary symmetric polynomials in $\theta_1, \theta_2, \theta_3, \theta_4, \theta_5$ are precisely the coefficients of the given polynomial.

In particular, $s_5 = \theta_1\theta_2\theta_3\theta_4\theta_5 = -5$ and $s_4 = \theta_1\theta_2\theta_3\theta_4 + \theta_1\theta_2\theta_3\theta_5 + \theta_1\theta_3\theta_4\theta_5 + \theta_1\theta_2\theta_4\theta_5 + \theta_2\theta_3\theta_4\theta_5 = 4$. Therefore $\sum_{i=1}^{i=5}(1/\theta_i) = s_4/s_5 = -4/5$.

Another solution: Note that $g(\theta) = 0$ if and only if $g(\theta)/\theta^5 = 0$, i.e., if and only if $1 + 2\theta^{-1} + 3\theta^{-2} + 4\theta^{-4} + 5\theta^{-5} = 0$, i.e., if and only if $1/\theta$ is a root of $1 + 2x + 3x^2 + 4x^4 + 5x^5$ or (equivalently) a root of the polynomial

$$h(x) = \frac{1}{5} + \frac{2}{5}x + \frac{3}{5}x^2 + \frac{4}{5}x^4 + x^5.$$

That is, the roots of $h(x)$ are precisely the reciprocals of the roots of $g(x)$. Since $h(x)$ is monic, the sum of its roots is minus the coefficient of x^4 . Thus the answer is $-\frac{4}{5}$.

3. Let K be a Galois extension of F . Suppose $[K : F]$ is divisible by p^m , where p is a prime number. (a). Prove that there is a field L such that $F \subset L \subset K$ and such that $[K : L] = p^m$.

Solution: We know that $|\text{Gal}(K/F)| = [K : F]$, so by the Sylow Theorems, there is a subgroup H of $\text{Gal}(K/F)$ with $|H| = p^m$. Let L be the field of elements that are fixed by H . Then by the Fundamental Theorem, $[K : L] = |H| = p^m$.

Note: One version of the Sylow Theorems states that if p^m divides the order of G , then G has a subgroup of order p^m . (This is the version quoted above.) Sometimes the theorem is only stated under the assumption that p^m is the highest power of p that divides $|G|$. However, any group of order p^n has subgroups of every order p^k for $k < n$, so this special case implies the general result.

(b). Suppose K is the splitting field of an irreducible polynomial $f(x) \in F[x]$. Let a be one of the roots of $f(x)$. Prove that the field L in part (a) may be chosen so that $a \notin L$.

Solution: Since $[K : L] > 1$, L is a proper subfield of K , so L does not contain all the roots of $f(x)$ (since K is a splitting field for $f(x)$, it is the smallest extension of F that contains all the roots of $f(x)$). Let b be a root of $f(x)$ that is not in L . We know that there is an automorphism $\phi \in \text{Gal}(K/F)$ such that $\phi(b) = a$. Since $b \notin L$, $a = \phi(b) \notin \phi(L)$. Thus $\phi(L)$ is a subfield of K such that $[K : \phi(L)] = [K : L] = p^m$ and such that $a \notin \phi(L)$. In other words, $\phi(L)$ is the desired subfield.

4(a). Suppose $K \subset \mathbb{R}$ is a Galois extension of L such that $[K : L]$ is an odd prime p . Suppose E and $E(r)$ are fields such that $[E(r) : E] = q$ for some prime number q and such that

$$(*) \quad K \cap E = L \neq K \cap E(r).$$

Prove that $q = p$ and that $E(r)$ is a Galois extension of E .

Solution: Let $E' = E(r)$. Note that

$$p = [K : L] = [K : K \cap E'] [K \cap E' : L].$$

Since p is prime, $[K \cap E' : L]$ equals 1 or p . By (*), it must equal p , so $[K : K \cap E'] = 1$ and therefore

$$K \subset E'.$$

Similarly,

$$q = [E' : E] = [E' : KE] [KE : E].$$

Since q is prime, $[KE : E]$ equals 1 or q . By (*), K is not contained in E , so $KE \neq E$ and $[KE : E] \neq 1$. Thus $[KE : E] = q$ and therefore $[E' : KE] = 1$, so

$$KE = E'.$$

By proposition 19 of section 14.4 of the text, $E' = KE$ is a Galois extension of E with $\text{Gal}(E'/E)$ isomorphic to $\text{Gal}(K/(K \cap E)) = \text{Gal}(K/L)$. Therefore

$$q = [E' : E] = |\text{Gal}(E'/E)| = [K : L] = p.$$

(b). Let K and L be as in part (a). Suppose that E and $E(r)$ are fields such that (*) holds and such that $r^q \in E$ for some prime number q . Prove that $E(r) \not\subset \mathbb{R}$.

Solution: Let $b = r^q$. By hypothesis, $q (= p)$ is odd. We may assume $E \subset \mathbb{R}$ since otherwise we're done. Note by (*) that $r \notin E$. Then it follows that q is the smallest integer such that $r^q \in E$. (In other words, $r^d \notin E$ for all $d < q$; see the solution to exercise 5a on the previous problem set for the proof of this fact). Then by hw7, problem 4, the minimal polynomial of r over E is $x^q - r^q$, so $[E(r) : E] = q$ and therefore the conclusions of part (a) hold. In particular, $E(r)/E$ is Galois, so $E(r)$ must contain all the roots of $x^q - r^q$. But since $q = p$ is odd, only one of those roots is real. Thus $E(r) \not\subset \mathbb{R}$.

(c). Let K and L be as in part (a). Prove that if $E \subset \mathbb{R}$ is any real root extension of L , then $E \cap K = L$.

Solution: If E is a real root extension of L . Then $E = L(r_0, r_1, \dots, r_n)$ where $r_i^{p_i} \in E_i$ where $E_i = L(r_0, \dots, r_{i-1})$. We may suppose that each p_i is prime (by inserting extra elements r_j if necessary) Note that $E_0 = L$ and that $E_{i+1} = E_i(r_i)$. By induction and by part (b), $E_i \cap K = L$ for all i .

(d). Let F be a subfield of \mathbb{R} , and let $f(x) \in F[x]$ be an irreducible polynomial all of whose roots are real. Let K be the splitting field and suppose that $[K : F]$ is not a power of 2 (i.e., that $[K : F]$ is divisible by an odd prime p .) Let a be one of the roots of $f(x)$. Prove that a is not contained in any real root extension of F .

Remark: If K is the splitting field over F of an irreducible polynomial $f(x) \in F[x]$, then the degree of $f(x)$ divides $[K : F]$. Thus if the degree of $f(x)$ has an odd factor, then so does $[K : F]$, and thus the conclusion of (d) holds.

Solution: By problem 3, there is a field L such that $F \subset L \subset K$ and such that $[K : L] = p$ and such that $a \notin L$. Since K/F is Galois, K/L is also Galois. By part (c), a is not contained in any real root extension of L . Thus it is not contained in any real root extension of F . (Any real root extension of F is contained in the corresponding real root extension of L .)

5. Express $f(x) = \sum_{i \neq j} x_i^2 x_j$ as a polynomial in the elementary symmetric polynomials. (See exercises 37 and 38 in section 14.6 of the text.)

Solution: The algorithm in 14.6 problems 37 and 38 is the following: consider the terms in $f(x)$ containing the highest possible power of x_1 . Of those terms, consider the ones containing the highest possible power of x_2 , and so on. The result is a single term $Ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ with $a_1 \geq a_2 \geq \cdots \geq a_n$. The algorithm tells us that

$$As_1^{a_1-a_2}s_2^{a_2-a_3}\cdots s_n^{a_n}$$

will be one of the terms in the expression for $f(x)$ as a polynomial in s_1, \dots, s_n .

In our case, the relevant term (the first term in the lexicographic ordering described in the text) is $x_1^2x_2$. Thus we write

$$f(x) = s_1^{2-1}s_2 + E(x) = s_1s_2 + E(x)$$

or

$$\begin{aligned} E(x) &= f(x) - s_1s_2 \\ &= \sum_{i \neq j} x_i^2 x_j - \left(\sum_i x_i \right) \left(\sum_{j < k} x_j x_k \right) \\ &= \sum_{i \neq j} x_i^2 x_j - \sum_{i < j < k} x_i x_j x_k - \sum_{j < k} x_j^2 x_k - \sum_{j < i < k} x_j x_i x_k - \sum_{j < k} x_j x_k^2 - \sum_{j < k < i} x_j x_k x_i \\ &= -3s_3. \end{aligned}$$

Thus $f(x) = s_1s_2 - 3s_3$.

Remark: In this example, the algorithm ended after one step because $E(x)$ turned out to be a scalar multiple of an elementary symmetric polynomial. In general, more than one step may be required.

6. Suppose $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree n with roots $\theta_1, \dots, \theta_n$. Prove that there is a monic polynomial $g(x) \in \mathbb{Z}[x]$ of degree n whose roots are $\theta_1^2, \dots, \theta_n^2$. (Indeed, given any $f(x)$, you can find the corresponding $g(x)$ even though you may not be able to find the roots of $f(x)$.)

Solution: Let's write $f(x) = \prod (x - \theta_i) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(x) = \prod (x - \theta_i^2) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. We know that $f(x) \in \mathbb{Z}[x]$ and we must show that $g(x) \in \mathbb{Z}[x]$.

Now, the coefficients of $g(x)$ are the elementary symmetric polynomials in $\theta_1^2, \theta_2^2, \dots, \theta_n^2$. It's clear that they are symmetric polynomials in $\theta_1, \theta_2, \dots, \theta_n$ and we know that any symmetric polynomial in $\theta_1, \theta_2, \dots, \theta_n$ can be expressed as a polynomial in a_0, a_1, \dots, a_{n-1} (i.e., the elementary symmetric polynomials in $\theta_1, \theta_2, \dots, \theta_n$). Therefore we conclude that there exists $p_0, p_1, \dots, p_{n-1} \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ such that $b_i = p_i(a_0, a_1, \dots, a_{n-1})$. Since $a_i \in \mathbb{Z}$ for all i (by assumption), it follows that $b_i \in \mathbb{Z}$ for all i . Thus, $g(x) \in \mathbb{Z}[x]$, as was to be shown.

7. (Not to turn in. For your enjoyment only.) Suppose K is a Galois extension of F such that $[K : F] = 2^n$ for some n . Then K is a root extension of F .

Solution: The assertion is false if the characteristic of F is 2, so the problem should have specified that F has characteristic not equal to 2.

Suppose first that $n = 1$. Then $K = F(\sqrt{D})$ for some $D \in F$. (See the discussion of quadratic extensions in 13.2 of the text.)

Now suppose $n > 1$. Now $\text{Gal}(K/F) = [K : F] = 2^n$, so from group theory we know that $\text{Gal}(K/F)$ has subgroups of order 2^k for every $k < n$. (We mentioned this fact in the proof of the fundamental theorem of algebra.) In particular, it has a subgroup H with $|H| = 2^{n-1}$. Let M be the corresponding fixed field. Then K is a Galois extension of M and $[K : M] = |G|/|H| = 2$. By the case $n = 1$, K is a root extension of M . By induction, M is a root extension of F , so we are done. \square