

MATH 121 MIDTERM SOLUTIONS

FEBRUARY 21, 2008

1. Prove that the polynomial $p(x) = x^5 + 12x^4 + 6x^3 + 6x + 18$ is irreducible in $\mathbb{Q}[x]$.

Solution: The leading coefficient is not divisible by 2, all the other coefficients are divisible by 2, and the constant term is not divisible by 4. Thus the polynomial is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion (with $p = 2$).

2. Find $[\mathbb{Q}(2^{1/5}, 3^{1/2}) : \mathbb{Q}]$.

Solution: For simplicity, let $K = \mathbb{Q}(2^{1/5}, 3^{1/2})$. On one hand, we know that $[K : \mathbb{Q}]$ is divisible by $[\mathbb{Q}(2^{1/5}) : \mathbb{Q}]$ (which is equal to 5) and also is divisible by $[\mathbb{Q}(3^{1/2}) : \mathbb{Q}]$ (which is equal to 2). Since 2 and 5 are coprime, it follows that $[K : \mathbb{Q}]$ is divisible by $2 \cdot 5 = 10$, so in particular, $[K : \mathbb{Q}] \geq 10$. On the other hand, $3^{1/2}$ has degree at most 2 over $\mathbb{Q}(2^{1/5})$ because it is a root of $x^2 - 3 \in \mathbb{Q}(2^{1/5})[x]$. Hence, since $[\mathbb{Q}(2^{1/5}) : \mathbb{Q}] = 5$ we see that $[K : \mathbb{Q}] \leq 5 \cdot 2 = 10$. Thus we conclude that $[K : \mathbb{Q}] = 10$.

3. Let E be a field and $K = E(x_1, x_2, x_3, x_4)$. Let $\sigma \in \text{Aut}(K/E)$ be the automorphism such that $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, $\sigma(x_3) = x_4$, and $\sigma(x_4) = x_1$. Let F be the set of elements of K that are fixed by σ .

Find the minimal polynomial $f(x) \in F[x]$ of the element x_1x_3 of K .

Solution: Note that K/F is a Galois extension with Galois group $\langle \sigma \rangle$ and hence the minimal polynomial of x_1x_3 is given by $\prod (x - y_i)$ where the product is over the elements in the orbit of x_1x_3 under the Galois group. We see that $\sigma(x_1x_3) = x_2x_4$ and $\sigma^2(x_1x_3) = x_1x_3$. Since σ^2 fixes x_1x_3 we see that there are only two elements in the orbit of x_1x_3 under the Galois group, namely x_1x_3 and x_2x_4 . Thus, the minimal polynomial is $(x - x_1x_3)(x - x_2x_4) = x^2 - (x_1x_3 + x_2x_4)x + x_1x_2x_3x_4 \in F[x]$.

4. Suppose K is a Galois extension of F and that H is a subgroup of $G = \text{Aut}(K/F)$. Answer the following questions (no proofs required):

(a). What is the field K_H associated to H under the pairing in the Fundamental Theorem of Galois Theory?

Solution: K_H consists of all elements of K which are fixed by every element of H . In other words, $K_H = \{k \in K : \sigma(k) = k \text{ for all } \sigma \in H\}$.

(b). What is the necessary and sufficient condition on H in order for K to be a Galois extension of K_H ?

Solution: K is always a Galois extension of K_H (and the Galois group is H).

(c). What is the necessary and sufficient condition on H in order for K_H to be a Galois extension of F ?

Solution: H must be a normal subgroup of the Galois group $\text{Gal}(K/F)$.

5. Let K be the splitting field of $x^4 - 3$ over \mathbb{Q} . Find $\text{Aut}(K/\mathbb{Q})$.

Solution: First, note that the four roots of this polynomial in \mathbb{C} are $\pm 3^{1/4}, \pm i3^{1/4}$. From this we see that $K = \mathbb{Q}(i, 3^{1/4})$ and that $[K : \mathbb{Q}] = 8$. (This is essentially the same as exercise 5 on problem set 3).

Since K is Galois over $\mathbb{Q}(3^{1/4})$, there exists an automorphism τ of K which fixes $\mathbb{Q}(3^{1/4})$ and maps i to $-i$. It's easy to check that τ^2 is the identity map.

We have a tower of fields $\mathbb{Q} \subset \mathbb{Q}(i) \subset K$ and from this we see that K must have degree 4 over $\mathbb{Q}(i)$. Thus, $3^{1/4}$ has degree 4 over $\mathbb{Q}(i)$, which implies that $x^4 - 3$ is irreducible over $\mathbb{Q}(i)$. Also, K is a Galois extension of $\mathbb{Q}(i)$. By exercise 2 on problem set 3, there exists an automorphism σ of K which fixes $\mathbb{Q}(i)$ and maps $3^{1/4}$ to $i3^{1/4}$. Then one can easily verify that σ has order 4 and that $\tau \notin \langle \sigma \rangle$. Since the Galois group has order 8 and since $\tau \notin \langle \sigma \rangle$ it follows that the Galois group is equal to $\langle \tau, \sigma \rangle$. Finally, it's easy to check that $\tau\sigma = \sigma^3\tau$ and this tells us that the Galois group $\text{Gal}(K/\mathbb{Q})$ is (isomorphic to) the dihedral group D_4 .

Another solution: As indicated above, $K = \mathbb{Q}(i, 3^{1/4})$. Now $3^{1/4}$ is a root of $x^4 - 3$, which is irreducible over \mathbb{Q} (by Eisenstein), so $[\mathbb{Q}(3^{1/4}) : \mathbb{Q}] = 4$. Now $\mathbb{Q}(3^{1/4}) \subset \mathbb{R}$, so $i \notin \mathbb{Q}(3^{1/4})$. Since i is a root of $x^2 + 1$, this means that $\mathbb{Q}(3^{1/4}, i)$ is a degree 2 extension of $\mathbb{Q}(3^{1/4})$. Thus $[\mathbb{Q}(3^{1/4}, i) : \mathbb{Q}] = [\mathbb{Q}(3^{1/4}, i) : \mathbb{Q}(3^{1/4})][\mathbb{Q}(3^{1/4}, i) : \mathbb{Q}] = 8$. Now the roots of $x^4 - 3$ are $r_1 = 3^{1/4}$, $r_2 = -3^{1/4}$, $r_3 = 3^{1/4}i$, and $r_4 = -3^{1/4}i$.

We know that $\text{Aut}(K/\mathbb{Q})$ is isomorphic to subgroup of the group of permutations of the roots, and therefore it is isomorphic to subgroup G of S_4 . Also, $|G| = [K : \mathbb{Q}] = 8$.

Since $x^4 - 3$ is irreducible over \mathbb{Q} , we know that for any two roots r_i and r_j , there is an isomorphism from $\mathbb{Q}(r_i)$ to $\mathbb{Q}(r_j)$ that maps r_i to r_j and that fixes elements of \mathbb{Q} . Since K is a splitting field, the isomorphism extends to an element of $\text{Aut}(K/\mathbb{Q})$. Thus $\text{Aut}(K/\mathbb{Q})$ is isomorphic to a transitive subgroup G of S_4 .

Now complex conjugation gives us one element of $\text{Aut}(K/\mathbb{Q})$. The corresponding element of S_4 is (12) (since conjugation switches r_1 and r_2 , leaving r_3 and r_4 fixed.)

We know there is at least one element of $\text{Aut}(K/\mathbb{Q})$ taking r_3 to r_4 . Since $r_3 + r_4 = 0$, it must then take r_4 to r_3 . Thus it must correspond either to (34) or to $(12)(34)$.

That is, G must contain at least one of these two elements. Since it also contains (12) , it must in fact contain both.

Likewise, $\text{Aut}(K/\mathbb{Q})$ must contain an automorphism that takes r_1 to r_3 . Again, since $r_1 + r_2 = r_3 + r_4$, it must then take r_2 to r_4 . It must also take r_3 to one of r_1 and r_2 and take r_4 to the other one. In other words, G must contain one of the following two elements: (1324) or $(13)(24)$. But then it must contain both since the first is the second multiplied by (12) , which is in G . The same reasoning shows that G must also contain (1423) and $(14)(23)$. But now we have found all 8 elements of G :

Identity,
(12), (34)
(12)(34), (13)(24), (14)(23)
(1324), (1423).

6. Let F be a field of characteristic 0 and let $p(x)$ be an irreducible polynomial in $F[x]$. Prove that $p(x)$ is separable.

Solution: Recall that a polynomial is separable if and only if it is relatively prime to its derivative. If $p(x)$ has degree n then its derivative $p'(x)$ has degree $n - 1$. Since $p(x)$ is irreducible, the only factors of $p(x)$ in $F[x]$ are 1 and $p(x)$. Hence we see that $p'(x)$ cannot be a multiple of $p(x)$ and hence must be coprime to $p(x)$ and thus $p(x)$ is separable.