Math 123 HW 11 Solutions

Eric Shen

April 2023

0.1 Small Note

It's important to justify that the maps you state indeed satisfy the properties you claim! In particular, many students lost marks because they said something was an automorphism without proof. Give some justification, especially because it might not be as obvious as you think.

Also, we require work to be shown for all problems, even if they begin with "**compute**"!

1 Problem 1

Author's Solution:

By the Primitive Element Theorem we may write $L = K(t)$ for some $t \in L$. Now, let the minimal polynomial of t over K be $p(x) = x^2 + ax + b$. Then the roots of p in $\overline{K} \supset L$ are $t, -a - t$ by Vieta's Formulas. But note that $-a - t \in K(t) = L$, so $L = K(t) = K(t, -a - t)$ is the splitting field of p. In particular, as shown in class, since L/K is a splitting field we hence know that $|Gal(L/K)| = [L : K] = 2$, so $Gal(L/K) \cong \mathbb{Z}/2$ (as this is the only group of order 2.

1.1 Remarks

- A common error was to directly consider a t for which $t \notin L, t^2 \in L$. In particular, many students just stated that if $t \in L - K$ then $t^2 \in L$ It is not immediately obvious why such a t exists (although you can retrieve one from the square root of the discriminant), and it is certainly not true that this is true for all $t \in L - K$ (for example, consider $\omega = e^{2\pi i/3}$ in $\mathbb{Q}(\omega)/\mathbb{Q}$.) We only know from $[L : K] = 2$ that for any $t \in L - K$, $\{1, t, t^2\}$ must be a *linearly dependent set*, which only implies the existence of some relation $t^2 + at + b = 0$ where $a, b \in K$.

2 Problem 2

Author's Solution:

Recall from HW 10 Problem 2 that $[L : \mathbb{Q}] = 4$. Hence $[L : \mathbb{Q}(\sqrt{2})] = [L : \mathbb{Q}(\sqrt{5})] = 2$. By problem 1 of this PSet we hence know that there exists a nontrivial $\alpha \in Gal(L/\mathbb{Q}(\sqrt{2}))$, $\beta \in Gal(L/\mathbb{Q}(\sqrt{5}))$, both of order 2. Since α, β are both automorphisms of L fixing $\mathbb{Q}$, we also find that $\alpha, \beta \in Gal(L/\mathbb{Q})$. Note also that $\alpha \neq \beta$, as if $\alpha = \beta$ then α fixes both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, and hence all of L (which contradicts the choice of α being nontrivial.) Hence $Gal(L/\mathbb{Q})$ has ≥ 2 elements of order 2. Also recall from class that $|Gal(L/\mathbb{Q})| \leq [L : \mathbb{Q}] = 4$, but the only group of order ≤ 4 with ≥ 2 elements of order 2 is $\mathbb{Z}/2 \times \mathbb{Z}/2$, so $Gal(L/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, as desired.

2.1 Remarks

- Remember that automorphisms are not roots! They're fundamentally different mathematical objects and should be considered as such. It is true that the automorphisms in $Gal(L/K)$ *permute* the roots in L of any polynomial in $K[x]$, as they commute with all polynomials in $K[x]$. It is also true that *given* a *primitive* element $t \in L/K$, the automorphisms are *determined* by which K-Galois conjugate they send t to. But they're not just roots! There are a lot of conditions here that need to be taken into account, and for the sake of clarity it is important to be as precise as possible with terminology.

3 Problem 3

Author's Solution:

Oops, apparently there is a very short solution to this problem.

Note that:

$$0 = \left(\sum_i a_i\right)\left(\sum_i a_i^2\right) = \sum_i a_i^3 + 2\sum_{i<j} a_i^2 a_j$$
$$0 = \left(\sum_i a_i\right)\left(\sum_{i<j} a_i a_j\right) = 2\sum_{i<j} a_i^2 a_j + 3\sum_{i<j<k} a_i a_j a_k$$

By Vieta's $\sum_{i<j<k} a_i a_j a_k = -1$, so $\sum_i a_i^3 = \boxed{-3}$.

3.1 Remarks

- People did very well on this problem!

4 Problem 4

Author's Solution:

By Artin 15.7.3 b),

- $x^3 - x$ is precisely the product of the irreducible polynomials of degree 1 in $\mathbb{F}_3[x]$.
- $x^{3^5} - x$ is precisely the product of the irreducible polynomials of degree 1 and 5 in $\mathbb{F}_3[x]$.

Thus the product of the irreducible polynomials of degree 5 is $\frac{x^{3^5}-x}{x^3-x}$, so the number of such polynomials is

$$\frac{1}{5}\deg\left(\frac{x^{3^5}-x}{x^3-x}\right) = \frac{240}{5} = \boxed{48}$$

4.1 Remarks

- People also did quite well on this problem.

5 Problem 5

Author's Solution:

$[L : K_1] = 2$ was shown in HW 9 Problem 5. Note that $L = \mathbb{C}(x) = \mathbb{C}(x-1)$, so by the substitution $x - 1 \mapsto x$ we analogously find $[L : K_2] = 2$. We now consider $K_1 \cap K_2$.

Consider any $p(x) \in K_1 \cap K_2$. Since $p(x) \in K_1 = \mathbb{C}(x^2)$, $p(x) = p(-x)$. Since $p(x) \in K_2 = \mathbb{C}((x-1)^2)$, $p(x) = p(2-x)$. So $p(x) = p(-x) = p(x+2)$. Now, let $p(0) = c$, and write $p(x) = \frac{f(x)}{g(x)}$ for $f, g \in \mathbb{C}[x]$. Then

$$p(x) - c = \frac{f(x) - cg(x)}{g(x)}$$

has ∞ many zeroes. Hence so does $f(x) - cg(x)$, so since $f(x) - cg(x)$ is a polynomial in $\mathbb{C}[x]$ it must be the zero polynomial. Hence $f(x) = cg(x)$, and so $p(x) = c$.

Hence this implies that $\mathbb{C} \subset K_1 \cap K_2 \subset \mathbb{C}$, so $K_1 \cap K_2 = \mathbb{C}$. Evidently this implies that $[L : K_1 \cap K_2] = [L : \mathbb{C}] = \infty$ (as e.g. $\{1, x, x^2, \ldots\}$ are all $\mathbb{C}$-linearly independent in L.)

5.1 Remarks

- $\mathbb{C}(x)$ is the field of *rational* functions in x, not just polynomials!
- I docked 2 points if you didn't demonstrate why periodic rational functions are constant, as I believe the proof of this is less obvious than you may think.