ALGEBRA 2. HOMEWORK 8

In problems below, Hom *denotes homomorphisms of commutative unital rings.*

Problem 1.– Let L/K be a field extension such that $L = K(\alpha)$ for an algebraic element $\alpha \in L$ such that degree of the minimal polynomial $\mathsf{m}_\alpha(x)$ is odd. Prove that $L = K(\alpha^2)$.

Problem 2.– Let L/K be a field extension. Assume we have two elements $\alpha, \beta \in L$, which are both algebraic over K. Prove that, if $\deg(\mathsf{m}_\alpha(x))$ and $\deg(\mathsf{m}_\beta(x))$ are coprime, then $\mathsf{m}_\alpha(x)$ is irreducible in $K(\beta)[x]$.

Problem 3.– Let L/K be an *algebraic* extension. Let $R \subset E$ be a subring containing K. Prove that R is a field.

Problem 4.– Let K be the splitting extension of $p(x) = x^5 - 7$ over $\mathbb{Q}$. Compute $[K : \mathbb{Q}]$.

Problem 5.– Determine the minimal polynomials, over $\mathbb{Q}$, of the following elements of $\mathbb{C}$. Here, $\iota^2 = -1$.

$$\text{(i) } \sqrt{2} + \sqrt{3}, \qquad \text{(ii) } \frac{1 + \iota\sqrt{3}}{2}, \qquad \text{(iii) } \iota + 5^{\frac{1}{3}}.$$

Problem 6.– Let $p \in \mathbb{Z}_{\geq 2}$ be a prime number. For any $m \in \mathbb{Z}_{\geq 0}$, prove that there is a unique sequence:

$$e^{(p)}(m) = (c_i)_{i \in \mathbb{Z}_{\geq 0}} \in \{0, 1, \ldots, p-1\}^{\mathbb{Z}_{\geq 0}}$$

such that $m = \sum_{i=0}^{\infty} c_i p^i$ (expansion in base p, note that $c_i = 0$ if $p^i > m$). Prove that the following factorization holds in $\mathbb{F}_p[x]$:

$$(1 + x)^m = \prod_{i=0}^{\infty} \left(1 + x^{p^i}\right)^{c_i}.$$

(*Hint: prove that in $\mathbb{F}_p(y)$, we have $(1+y)^p = 1 + y^p$. See how c_i will change if both sides of the equation are multiplied by $(1 + x)$. Then show that the same rule gives the entries of $e_i^{(p)}(m+1)$ from those of $e_i^{(p)}(m)$.*)

Use the equation above to prove the following identity. For $m, n \in \mathbb{Z}_{\geq 0}$, let $e^{(p)}(m) = (c_i)$ and $e^{(p)}(n) = (d_i)$. Then we have:

$$\binom{m}{n} = \prod_{i=0}^{\infty} \binom{c_i}{d_i} \pmod{p},$$

where, our convention is $\binom{0}{0} = 1$ and $\binom{k}{\ell} = 0$, if $k < \ell$.

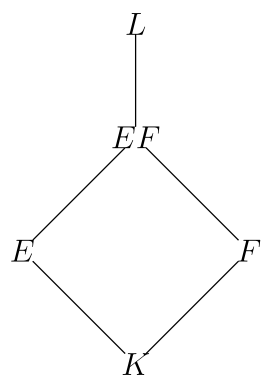
Problem 7.– For $a \in \mathbb{Z}$ consider the polynomial $f_a(x) = x^4 - ax - 1 \in \mathbb{Z}[x]$. Prove that if $a \neq 0$, then $f_a(x)$ is irreducible in $\mathbb{Q}[x]$. Consider the field $K_a = \mathbb{Q}[x]/(f_a(x))$. Prove that there are infinitely many $a \in \mathbb{Z}_{\neq 0}$ such that: $\boxed{\mathbb{Q} \subset E \subset K_a \Rightarrow E = \mathbb{Q} \text{ or } E = K_a}$, where E is a subextension of $\mathbb{Q} \subset K_a$.

Problem 8.– Verify that $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible. Let $K = \mathbb{Q}[x]/(x^3 - 2)$. Prove that $\mathrm{Hom}(K, \mathbb{C})$ has exactly 3 elements.

Problem 9.– Let K be a field and $L = K(t)$ be the field of rational functions of one variable t with coefficients from K. Prove that $L^{\mathrm{alg}} = K$.

Problem 10.– Let L/K be an algebraic extension. Prove that (i) if $|K| < \infty$, then L is at most countable; (ii) if K is countable, then L is countable. Deduce that there are uncountably many transcendental real numbers.

Definition.– Let L/K be a field extension and assume $E, F \subset L$ are two subfields containing K. Let $EF \subset L$ be the smallest subfield containing both E and F, called *the composite extension.*



We say E and F are *linearly disjoint* if the multiplication map:

$$\mu : E \otimes_K F \to L, \qquad \mu(e \otimes f) = ef, \ \forall\, e \in E, f \in F,$$

is injective.

Problem 11.– Assuming both E and F are finite over K, prove that

$$[EF : K] \leq [E : K] \cdot [F : K].$$

Prove that if $\gcd([E : K], [F : K]) = 1$, then this is an equality.

Problem 12.– Prove that E and F are linearly disjoint if and only if for every basis $\{\alpha_i\}_{i \in I}$ (resp. $\{\beta_j\}_{j \in J}$) of E (resp. F) over K, $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$ is is a basis of EF over K.

Problem 13.– Assume that there exist $\alpha, \beta \in L$, algebraic over K, such that $E = K(\alpha)$, $F = K(\beta)$, and $\mathsf{m}_\alpha(x) = \mathsf{m}_\beta(x)$. Show that E and F are not linearly disjoint.

Problem 14.– In the set up of Problem 2, prove that $K(\alpha)$ and $K(\beta)$ are linearly disjoint. Use this to give an example of a pair of linearly disjoint subextensions when $K = \mathbb{Q}$ and $L = \mathbb{C}$.