Álgebra moderna, ago-dic, 2019, CIMAT.

Problemas de práctica para el examen final

(Fecha del examen: 10 dic, 2019)

2.1. Which of the following subsets of $\mathbb{C}$ are fields with respect to the usual addition and multiplication of numbers:

(a) $\mathbb{Z}$;
(b) $\{0, 1\}$;
(c) $\{0\}$;
(d) $\{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$;
(e) $\{a + b\sqrt[3]{2},\ a, b \in \mathbb{Q}\}$;
(f) $\{a + b\sqrt[4]{2}, a, b \in \mathbb{Q}\}$;
(g) $\{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$;
(h) $\{z \in \mathbb{C} : |z| \leq 1\}$.

2.2. Show that every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

2.3. Give an example of an infinite field of characteristic $\neq 0$.

2.6. Give a description of all numbers belonging to the fields:

(a) $\mathbb{Q}(\sqrt{2})$; (b) $\mathbb{Q}(i)$; (c) $\mathbb{Q}(\sqrt{2}, i)$; (d) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2.7. Show that

(a) $\mathbb{Q}(\sqrt{5}, i\sqrt{5}) = \mathbb{Q}(i, \sqrt{5})$;
(b) $\mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
(c) $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$;
(d) $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, when $a, b \in \mathbb{Q}$, $\sqrt{a} + \sqrt{b} \neq 0$.

2.8. Give a description of the following subfields of $\mathbb{C}$:

(a) $\mathbb{Q}(X)$, where $X = \{\sqrt{2}, 1 + 2\sqrt{8}\}$;
(b) $\mathbb{Q}(i)(X)$, where $X = \{\sqrt{2}\}$;
(c) K_1K_2, where $K_1 = \mathbb{Q}(i)$, $K_2 = \mathbb{Q}(\sqrt{5})$;
(d) $\mathbb{Q}(X)$, where $X = \{z \in \mathbb{C} : z^4 = 1\}$.

4.2. (a) Show that if $f \in K[X]$ is irreducible over K and $L \supseteq K$ is a field extension such that the degree $\deg f$ and the degree $[L : K]$ are relatively prime, then f is irreducible over L.

4.3. Find the minimal polynomial and the degree of α over K when:

(a) $K = \mathbb{Q}$, $\alpha = \sqrt[3]{\sqrt{3} + 1}$;
(b) $K = \mathbb{Q}$, $\alpha = \sqrt{2} + \sqrt[3]{2}$;
(c) $K = \mathbb{Q}$, $\alpha^5 = 1$, $\alpha \neq 1$;
(d) $K = \mathbb{Q}(i)$, $\alpha = \sqrt{2}$;
(e) $K = \mathbb{Q}(\sqrt{2})$, $\alpha = \sqrt[3]{2}$;
(f) $K = \mathbb{Q}$, $\alpha^p = 1$, $\alpha \neq 1$, p a prime number.

4.4. Find the degree and a basis of the following extensions $L \supseteq K$:

(a) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, i)$;
(b) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
(c) $K = \mathbb{Q}$, $L = \mathbb{Q}(i, \sqrt[3]{2})$;
(d) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2} + 2\sqrt[3]{4})$;
(e) $K = \mathbb{R}(X + \frac{1}{X})$, $L = \mathbb{R}(X)$;
(f) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$;
(g) $K = \mathbb{Q}(\sqrt{3})$, $L = \mathbb{Q}(\sqrt[3]{1 + \sqrt{3}})$;
(h) $K = \mathbb{F}_2$, $L = \mathbb{F}_2(\alpha)$, where $\alpha^4 + \alpha^2 + 1 = 0$;
(i) $K = \mathbb{F}_3$, $L = \mathbb{F}_3(\alpha)$, where $\alpha^3 + \alpha^2 + 2 = 0$;
(j) $K = \mathbb{R}(X^2 + \frac{1}{X^2})$, $L = \mathbb{R}(X)$.

4.5. Show that a complex number $z = a + bi$ is algebraic (over $\mathbb{Q}$) if and only if a and b are algebraic.

4.6. Show that the numbers $\sin r\pi$ and $\cos r\pi$ are algebraic if r is a rational number.

4.7. Let $L = \mathbb{Q}(\sqrt[3]{2})$. Find $a, b, c \in \mathbb{Q}$ such that $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ when

(a) $x = \dfrac{1}{\sqrt[3]{2}}$; (b) $x = \dfrac{1}{1+\sqrt[3]{2}}$; (c) $x = \dfrac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}$.

4.8. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find $a, b, c, d \in \mathbb{Q}$ such that $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ when

(a) $x = \dfrac{1}{\sqrt{2}+\sqrt{3}}$; (b) $x = \dfrac{1}{1+\sqrt{2}+\sqrt{3}}$; (c) $x = \dfrac{\sqrt{2}+\sqrt{3}}{1+\sqrt{2}+\sqrt{3}+\sqrt{6}}$.

4.9. Let $L = \mathbb{F}_2(\alpha)$, where $\alpha^4+\alpha+1 = 0$. Find $a, b, c, d, \in \mathbb{F}_2$ such that $x = a+b\alpha+c\alpha^2+d\alpha^3$ when

(a) $x = \dfrac{1}{\alpha}$; (b) $x = \alpha^5$; (c) $x = \alpha^{15}$; (d) $x = \dfrac{1}{\alpha^2+\alpha+1}$.

4.14. Is it true that for each divisor d to $[L : K]$ there exists a field M between K and L such that $[M : K] = d$?

4.15. It is (well-)known that the numbers e and π are transcendental. It is not known whether $e+\pi$ and $e\pi$ are transcendental. Show that at least one of the numbers $e+\pi$ or $e\pi$ must be transcendental.

4.16. (a) Let $K \subseteq L$ be a field extension and let $f(\alpha) = 0$, where $\alpha \in L$ and $f(X)$ is a polynomial whose coefficients are algebraic over K. Prove that α is also algebraic over K.

(b) Assume that the number α is algebraic. Prove that also the following numbers are algebraic:

(b_1) α^2; (b_2) $\sqrt{\alpha}$; (b_3) $\sqrt[3]{1+\sqrt{\alpha}}$.

5.1. Find the degree and a basis of the splitting field over K for $f \in K[X]$ when

(a) $K = \mathbb{Q}$, $f = (X^2-2)(X^2-5)$;
(b) $K = \mathbb{Q}$, $f = X^3-2$;
(c) $K = \mathbb{Q}$, $f = X^4-2$;
(d) $K = \mathbb{Q}$, $f = X^4+X^2-1$;
(e) $K = \mathbb{Q}$, $f = X^4+1$;
(f) $K = \mathbb{Q}(i)$, $f = X^4-2$;
(g) $K = \mathbb{Q}(i)$, $f = (X^2-2)(X^2-3)$;
(h) $K = \mathbb{Q}$, $f = X^p-1$, p a prime number.

5.2. Decide whether the following pairs of fields are isomorphic:

(a) $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i\sqrt[4]{2})$;
(b) $\mathbb{Q}(\sqrt[3]{1+\sqrt{3}})$ and $\mathbb{Q}(\sqrt[3]{1-\sqrt{3}})$;
(c) $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

5.3. Let L be a splitting field of a polynomial $f(X)$ of degree n with coefficients in a field K. Show that $[L:K] \leq n!$.

5.4. Prove that a field with p^n elements contains a field with p^m elements if and only if $m|n$.

5.5. (a) Let $f(X)$ be an irreducible polynomial of degree n over a field $\mathbb{F}_p$. Show that $\mathbb{F}_p[X]/(f(X))$ is a field with p^n element, which is isomorphic with the splitting field of the polynomial $X^{p^n} - X$ and $f(X)$ divides $X^{p^n} - X$.

(b) Let $f(X)$ be an irreducible polynomial in $\mathbb{F}_p[X]$. Show that $f(X)|X^{p^n} - X$ if and only if $\deg(f(X))|n$.

6.1. Let $L \supseteq K$ be a field extension.

(a) Show that if $\alpha \in L$ is a zero of $f \in K[X]$ and $\sigma \in G(L/K)$, then $\sigma(\alpha)$ is also a zero of f.

(b) Show that if $L = K(\alpha_1, \ldots, \alpha_r)$ and two automorphisms $\sigma, \tau \in G(L/K)$ are equal for every generator α_i (that is, $\sigma(\alpha_i) = \tau(\alpha_i)$ for each i), then $\sigma = \tau$ (that is, $\sigma(\alpha) = \tau(\alpha)$ for every $\alpha \in L$).

9.1. Which of the following extensions $L \supseteq K$ are Galois?

(a) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$;
(b) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[4]{2})$;
(c) $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$;
(d) $K = \mathbb{Q}(i)$, $L = \mathbb{Q}(i, \sqrt[4]{2})$;
(e) $K = \mathbb{Q}(X^2)$, $L = \mathbb{Q}(X)$;
(f) $K = \mathbb{F}_p(X^2)$, $L = \mathbb{F}_p(X), p$ a prime number;
(g) $K = \mathbb{F}_2(X^2 + X)$, $L = \mathbb{F}_2(X)$;
(h) $K = \mathbb{R}(X^3)$, $L = \mathbb{R}(X)$.

9.2. Find all subgroups of the Galois group $G(L/K)$ of the splitting field L of the polynomial f as well as all corresponding subfields M between K and L when

(a) $K = \mathbb{Q}, f(X) = (X^2-2)(X^2-5)$;
(b) $K = \mathbb{Q}, f(X) = (X^4-1)(X^2-5)$;
(c) $K = \mathbb{Q}, f(X) = X^5 - 1$;
(d) $K = \mathbb{Q}, f(X) = X^4 + 1$;
(e) $K = \mathbb{Q}(i), f(X) = X^4 - 2$;
(f) $K = \mathbb{Q}, f(X) = X^3 - 5$;
(g) $K = \mathbb{Q}, f(X) = X^4 + X^2 - 1$;
(h) $K = \mathbb{Q}(i), f(X) = X^3 - 1$.

9.3. (a) Let $f(X) \in K[X]$ be a polynomial of degree n over a field K and let $K_f = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field of $f(X)$ over K, where α_i are all zeros of $f(X)$ in K_f. Show that the permutations σ of the indices i of the zeros α_i corresponding to the automorphisms $\sigma \in G(L/K)$ according to $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ form a subgroup of S_n.

(b) Give a description of the Galois group $G(K_f/K)$ as a permutation subgroup of S_n ($n = \deg f$) for polynomials $f(X)$ in Ex. 9.2.

9.5. Show that the extension $L \supseteq K$ is Galois, find the Galois group $G(L/K)$, all its subgroups and the corresponding subfields between K and L when

(a) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, i)$;
(b) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon), \varepsilon^3 = 1, \varepsilon \neq 1$;
(c) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2}, i)$;
(d) $K = \mathbb{R}(X^2 + \frac{1}{X^2}), L = \mathbb{R}(X)$;
(e) $K = \mathbb{R}(X^2, Y^2), L = \mathbb{R}(X, Y)$;
(f) $K = \mathbb{R}(X^2 + Y^2, XY), L = \mathbb{R}(X, Y)$.

9.6. Is it true that if $L \supseteq M$ and $M \supseteq K$ are Galois extensions, then $L \supseteq K$ is a Galois extension?