

FIELD THEORY PROBLEM SET #3

MATHCAMP 2003

1. (a) Suppose that K is a field, and K' is a set with two operations, addition (which we will denote $+$) and multiplication (which we will denote \cdot). Suppose that there exists a function $f : K \rightarrow K'$ which is one-to-one and onto, and such that if $x, y \in K$, then $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x) \cdot f(y)$. Prove that K' is a field under $+$ and \cdot .
(b) If $d \in \mathbb{Q}$ is a non-square, give a suitable function from $\mathbb{Q}[x]/\langle x^2 - d \rangle$ to $\mathbb{Q}(\sqrt{d})$, and use part (a) to conclude that $\mathbb{Q}(\sqrt{d})$ is a field.
(c) Give a suitable function from $\mathbb{Q}[x]/\langle x^3 - 2 \rangle$ to $\mathbb{Q}(\sqrt[3]{2})$, and use part (a) to conclude that $\mathbb{Q}(\sqrt[3]{2})$ is a field.
(d) Suppose that $\alpha \in \mathbb{C}$ is an algebraic number of degree n . Let $\mathbb{Q}(\alpha)$ be the set $\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\}$. Show that $\mathbb{Q}(\alpha)$ is a field.
2. (a) Can you construct a field with exactly 9 elements? Exactly 25 elements? Exactly 27 elements?
(b) Prove that if there exists a field containing exactly q elements, then q must be a prime power.
3. (a) Find the minimal polynomial over \mathbb{Q} of $\sqrt{1 + \sqrt[3]{2}}$.
(b) Prove that $x^5 - 7$ is irreducible over \mathbb{Q} . Find the minimal polynomial over \mathbb{Q} of the element $x^2 + x \in \mathbb{Q}[x]/\langle x^5 - 7 \rangle$.
4. (a) Show that the polynomial $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and use this to prove that the degree $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is exactly 4.
(b) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} , and use this to give another proof that the degree $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is exactly 4.
(c) Find a polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(\sqrt{2} + \sqrt{3}) = \sqrt{2}$.
5. Suppose that V is a vector space of dimension n over K , and suppose that $v_1, \dots, v_n \in V$ are linearly independent. Prove that they are a basis of V . (Hint: we need to show that v_1, \dots, v_n span V , so suppose that $v \in V$ cannot be written as a linear combination of v_1, \dots, v_n . Show that v, v_1, \dots, v_n are linearly independent, and use this to derive a contradiction.)