MA3D5 Galois Theory – Sheet 2

Deadline: Thursday, 7 February 2008, 3:00.

Solutions to Section B are for handing in. Please put your solutions into the MA3D5 Galois Theory box in front of the Undergraduate Office. Mention your department if it is not mathematics.

(A1) Let K be a field, A a nonzero ring, $f\colon K \to A$ a ring homomorphism.

(a) Prove that f is injective. Note: by definition, we have $f(1_K) = 1_A$. One often writes $f(t)$ instead of t if $t \in K$, and calls A a K-algebra.

(b) Prove that A becomes a vector space over K on defining addition in (the vector space) A to be addition in (the ring) A, and scalar multiplication to be $(t, u) \mapsto (f(t))\, u$ ($t \in K$, $u \in A$).

(c) Let $a \in A$. Prove that the map $A \to A$, $u \mapsto au$ is K-linear.

(A2) Let a denote the image of x in $\mathbb{Q}[x]/(x^3 + 3x + 3)$. Express each of $1/a$, $1/(1 + a)$ and $1/(1 + a^2)$ in the form $c_2a^2 + c_1a + c_0$ with $c_i \in \mathbb{Q}$.

(B1) Let A be a ring of characteristic p (a prime number).

(a) Prove that $F\colon A \to A$ defined by $F(a) = a^p$ is a ring homomorphism. Hint: One of the things you need to prove is that most coefficients in the binomial theorem for $(x + y)^p$ are divisible by p.

(b) Prove $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$ ($a_i \in A$).

(c) Prove Fermat's theorem that $p \mid n^p - n$ for all integers n.

(B2) Consider the polynomials $f = x^5 + x^2 + 3$, $g = x^3 + 2$ over $\mathbb{Q}$. Using the Euclidean algorithm, find $p, q \in \mathbb{Q}[x]$ such that $pf + qg = 1$, with q of degree ≤ 4. Find $h \in \mathbb{Q}[x]$ such that if $f(\alpha) = 0$ (that is, α is a root of f in some field extension) then $h(\alpha) = g(\alpha)^{-1}$.

(B3) Let K be a field. Let $f \in K[x]$ be a polynomial of degree n. Put $A = K[x]/(f)$ and let $p\colon K[x] \to A$, $p(g) = g + (f)$ be the natural map. Put $\alpha := p(x)$. Recall from (A1) that A is a K-vector space.

Prove that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a K-basis for A.

(B4) (a) Prove that $r := x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible. (Hint: if reducible, it must have a linear or quadratic factor. Try them all.) Using theorem 2.35 deduce that the lift $x^5 + x^2 + 3 \in \mathbb{Q}[x]$ is irreducible.

(b) Prove that $f := x^7 + 6\,x^3 + 12 \in \mathbb{Z}[x]$ is Eisenstein. Deduce that it is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

(c) Prove that $g := 2\,x^{10} + 4\,x^5 + 3 \in \mathbb{Q}[x]$ is irreducible. Hint: which related polynomial is Eisenstein? Use the result of (B5).

(d) Prove that $h := x^3 + 2\,x - 5 \in \mathbb{Z}[x]$ is irreducible.

(e) Prove that $s := x^{12} + x + 2$ has no roots in $\mathbb{Q}$. Hint: Use part (i) of Gauss' lemma 2.34.

(B5) Let K be a field. Let $a, b, c, d \in K$ be such that $ad - bc \neq 0$. Let $f \in K[x]$ be a polynomial of degree n.

(a) Prove that the expression

$$g(x) := (cx + d)^n \, f\Big(\frac{ax + b}{cx + d}\Big)$$

is in $K[x]$ and of degree $\leq n$.

(b) Prove that f is irreducible of degree n if and only if g is irreducible of degree n.

(C1) Let A be a finite integral domain. Prove that A is a field.

(C2) Let $L \supset K$ be a field extension such that $[L : K] = 2$.

(a) If K has characteristic 2, prove that there exists $\beta \in L \smallsetminus K$ such that $\beta^2 \in K$ or $\beta^2 + \beta \in K$. Hint: use (B3).

(b) If K has characteristic $\neq 2$, prove that there exists $\beta \in L \smallsetminus K$ such that $\beta^2 \in K$.

(C3) Let A be an integral domain containing a field K. Let $a \in A$. Recall from (A1) that A is a vector space over K and that the map

$$\begin{aligned} m_a \colon A &\longrightarrow A, \\ x &\longmapsto ax \end{aligned}$$

is K-linear. Assume that A has finite K-dimension.

(a) Prove that m_a is injective.

(b) Prove that m_a is surjective.

(c) Prove that A is a field.

(C4) In the lectures, we computed the irreducible polynomials in $\mathbb{F}_2[x]$ of degree ≤ 4. Compute those of degree 5.

(C5) Prove that the polynomial ring $K[x]$ over any field K has infinitely many irreducible polynomials. Hint: Imitate Euclid's proof that there are infinitely many prime numbers.

(D1) Let $f \colon \mathbb{R} \to \mathbb{R}$ be a ring homomorphism. Prove that f is the identity. (You may use that $f(1) = 1$ but not that f is continuous). This result is quite curious, since there are uncountably many homomorphisms $\mathbb{C} \to \mathbb{C}$.