MA3D5 Galois Theory – Sheet 2

Deadline: Thursday, 5 February 2008, 3:00.

Question (2.5) is not 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.

(2.1) Let A be an integral domain. Put

$$B = \big\{(a,b) \in A \times A \;\big|\; b \neq 0\big\}$$

and let $\sim$ be the binary relation on B defined by $(a,b) \sim (c,d)$ if and only if $ad = bc$.

(a) Prove that $\sim$ is an equivalence relation. We denote the equivalence class of (a,b) by a/b.

(b) Prove that the following are well-defined operations on $A/\!\sim$:

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a\,c}{b\,d}, \qquad \frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}.$$

Prove that this makes $A/\!\sim$ into a field. It is called the **field of fractions** of A and sometimes written $\operatorname{Frac} A$.

(c) What goes wrong in the above if A is a ring which is not an integral domain?

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

(a) Prove that the binomial coefficient $\binom{p}{k}$ is divisible by p if $0 < k < p$.

(b) Prove that $F\colon A \to A$ defined by $F(a) = a^p$ is a ring homomorphism. It is called the **Frobenius ring homomorphism**. Hint: use the binomial theorem.

(c) Is F necessarily injective? Surjective? Give a proof or a counterexample.

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

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

(2.3) 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 $h(\alpha) = g(\alpha)^{-1}$.

(2.4) (a) Prove that $h := X^3 + 6\,X - 11 \in \mathbb{Z}[X]$ is irreducible. Hint: Use Gauss' lemma.

(b) Prove that $s := X^{13} + X^{10} + X^7 + X^4 + 1$ has no roots in $\mathbb{Q}$. Hint: Use Gauss' lemma.

(c) 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.) Deduce that the lift $X^5 + X^2 + 3 \in \mathbb{Q}[X]$ is irreducible.

(d) 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 $\mathbb{Q}[X]$.

(e) 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 exercise (2.5) below.

(f) Prove that $X^8 + (Y^4 - 1)\,X^3 + (Y^4 - Y)$ is irreducible in $\mathbb{Q}(Y)[X]$.

(2.5) (Not for handing in). 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 $n > 1$.

(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 if and only if g is irreducible of degree n.