MA3D5 Galois theory

Assignment B

Deadline: Thursday of Week 4, Thu 29th Jan 2004.

B.1. In the proof of Proposition 2.4, write out the definition of addition and multiplication of fractions $\frac{a}{b}$, and run through the proof that addition is well defined (that is, it respects the equivalence relation defining the field of fractions $\operatorname{Frac} A$).

B.2. For $f, g \in k[x]$, the ideal $(f, g) \subset k[x]$ is generated by a single element $h \in k[x]$ by Corollary 2.24. Define $\operatorname{hcf}(f, g) = h$ (defined up to multiplication by a scalar in k). Show that h has the usual properties of hcf.

If division with remainder gives $f = qg + r$ with $\deg r < \deg g$, show that $\operatorname{hcf}(f, g) = \operatorname{hcf}(g, r)$. Show how to compute $\operatorname{hcf}(f, g)$ by the Euclidean algorithm. For

$$f = x^5 - 3x^2 + 2 \quad \text{and} \quad g := x^3 - 1,$$

calculate $\operatorname{hcf}(f, g)$, and find $a, b \in k[x]$ for which $h = af + bg$.

B.3. Let $k \subset K$ be a field extension and $\alpha \in K$ an algebraic element. Show how to calculate α^{-1} as a polynomial in α, given the minimal polynomial of α. (That is, write α^{-1} without denominator, as an element of the ring $k[\alpha]$, cf. Proposition 2.29.)

Suppose that $f = x^3 + ax + b$ is irreducible, and that $k \subset k[\alpha]$ where α is a root of f. Determine the minimal polynomial of $\alpha - 1$, and show how to write $(\alpha - 1)^{-1}$ as a polynomial expression in α.

B.4. Exam-style question

(A) Say what is an Eisenstein polynomial $f \in \mathbf{Z}[x]$ (for a prime p), and prove that an Eisenstein polynomial is irreducible over $\mathbf{Q}$.

(B) Let $f = 27x^3 - 9x^2 - 54x + 47$. Find a substitution $x = ay + b$ such that $f(ay + b)$ is an Eisenstein polynomial for a suitable prime, and deduce that f is irreducible. [Hint: There is no method, you just have to try something.]

Erratum Question P1 on Assignment A is too hard. (Thanks to the guy who pointed it out.) It asks for the elementary symmetric functions Σ_i of $\alpha_1^2, \dots, \alpha_n^2$ in terms of those of $\alpha_1, \dots, \alpha_n$. This is only reasonable for $n = 2$ or $n = 3$, or for the first or second elementary symmetric function.

You can do the question by elementary symmetric functions if you are really determined and use computer algebra to help guess the answer:

$$\Sigma_k := \sigma_k(\{\alpha_i^2\}) = \sigma_k^2 + 2\sum_{i=0}^{k-1}(-1)^{k-i}\sigma_i\sigma_{2k-i}, \tag{1}$$

$$\text{that is,}\quad \begin{aligned} &\Sigma_1 = \sigma_1^2 - 2\sigma_2, \quad \Sigma_2 = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4, \\ &\Sigma_3 = \sigma_3^2 - 2\sigma_2\sigma_4 + 2\sigma_1\sigma_5 - 2\sigma_6, \\ &\Sigma_4 = \sigma_4^2 - 2\sigma_3\sigma_5 + 2\sigma_2\sigma_6 - 2\sigma_1\sigma_7 + 2\sigma_8, \quad \text{etc.} \end{aligned}$$

A better solution: the polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0$ for x is the characteristic polynomial of

$$M := \begin{pmatrix} 0 & 1 & & \dots \\ & 0 & 1 & \dots \\ \vdots & & & \vdots \\ & & 0 & 1 \\ -a_n & -a_{n-1} & \dots & -a_1 \end{pmatrix};$$

M corresponds to multiplication by x on $\{1, x, \dots, x^{n-2}, x^{n-1}\}$, viewed as column vector. Multiplication by x^2 corresponds to

$$M^2 = \begin{pmatrix} 0 & 0 & 1 & & \dots \\ & 0 & 0 & 1 & \dots \\ \vdots & & & & \vdots \\ & & 0 & 0 & 1 \\ -a_n & -a_{n-1} & & \dots & -a_1 \\ a_1a_n & a_1a_{n-1} - a_n & & \dots & a_1^2 - a_2 \end{pmatrix}.$$

Now the equation for x^2 is the characteristic polynomial of M^2, that is $\det(M^2 - tI)$; it has coefficients given by (1).