Nepal Algebra Project 2017

Tribhuvan University

Module 1 — Problem Set 1 (MW)

These problems are due Sunday, May 7, 2017 at 10 pm Nepal time.
Send your solutions (including your name and email address) to `nap@rnta.eu` with a copy to `michel.waldschmidt@imj-prg.fr`

1. Let a, b, c, d belong to domain R and satisfy $a + b = c$. Assume d divides two of the elements a, b, c; prove that d divides the third.

2. Show that an integral domain with a finite number of elements is a field.

3. **(a)** Write the Euclidean algorithm to compute the gcd D of the two polynomials $A(X) = X^5 + 4X^3 + 3X$ and $B(X) = X^4 + 3X^2 + 1$ in $\mathbb{Q}[X]$.
(b) Deduce one Bézout relation $AU_0 + BV_0 = D$ with U_0 and V_0 in $\mathbb{Q}[X]$.
(c) Deduce all Bézout relations $AU + BV = D$ with U and V in $\mathbb{Q}[X]$.

4. Factor the polynomial $X^4 - 2X^2 + 9$ into irreducible polynomials
- over $\mathbb{C}$;
- over $\mathbb{R}$;
- over $\mathbb{Q}$.

5. **(a)** Let S be a ring, R a subring of S, $\alpha_1, \dots, \alpha_n$ elements in S. Denote by ψ the map from the ring of polynomials $R[X_1, \dots, X_n]$ to S which maps $f(X_1, \dots, X_n)$ to $f(\alpha_1, \dots, \alpha_n)$. Check that the image of ψ is the smallest subring of S containing R, $\alpha_1, \dots, \alpha_n$. This ring is denoted $R[\alpha_1, \dots, \alpha_n]$: it is the subring of S generated by $\alpha_1, \dots, \alpha_n$ over R.

(b) Let L be a field, K a subfield of S, $\alpha_1, \dots, \alpha_n$ elements in S. Check that the smallest subfield containing K, $\alpha_1, \dots, \alpha_n$ is the set of elements in L of the form $f(\alpha_1, \dots, \alpha_n)/g(\alpha_1, \dots, \alpha_n)$, where f and g run over the elements in $K[X_1, \dots, X_n]$ such that $g(\alpha_1, \dots, \alpha_n) \neq 0$. This field is denoted $K(\alpha_1, \dots, \alpha_n)$: it is the subfield of L generated by $\alpha_1, \dots, \alpha_n$ over K.

6. Let L be a field, K a subfield of L, $\alpha \in L$. Check that the following properties are equivalent
(i) α is algebraic over K;
(ii) $K(\alpha) = K[\alpha]$;
(iii) $K[\alpha]$ is a field;
(iv) $K[\alpha]$ is a finite dimensional vector space over K;
(v) $K(\alpha)$ is a finite dimensional vector space over K;
(vi) $1/\alpha \in K[\alpha]$.

7. Check that the subring E of $\mathbb{C}$ generated by $i, \sqrt{2}$ over $\mathbb{Q}$ is a field. Give a basis of E as a $\mathbb{Q}$–vector space. Find an element $\alpha \in E$ such that $E = \mathbb{Q}[\alpha]$ and write the irreducible polynomial of α over $\mathbb{Q}$.

8. Let F a field of characteristic p prime.
(a) Check that the polynomial $X^p - X$ has p roots in F. What is the set of these roots?
(b) Let r be a positive integer; set $q = p^r$. Show that the set of roots in F of the polynomial $X^q - X$ is a subfield of F, with p^s elements where $s \leq r$.
`Example`: assume F is a finite field with 4 elements, take $p = 2$, $r = 3$; compute s.

You can download Milne's book at: `http://www.jmilne.org/math/CourseNotes/FT.pdf`
The NAP website is: `http://www.rnta.eu/nap/nap-2017/`
Feel free to send an email anytime with questions about the course or the homework, or about other mathematical issues!