# Nepal Algebra Project 2017

Tribhuvan University

Module 1 — Problem Set 2 (MW)

These problems are due Tuesday, May 16, 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.** Prove that a finite subgroup of the multiplicative group of a field is cyclic.
`Hint`: this is Milne exercise 1.3.

**2.** Let $G$ be a cyclic group of order $n$ and let $m$ a positive integer. Prove that there exists a subgroup of $G$ of order $m$ if and only if $m$ divides $n$. Prove also that in this case, this subgroup of order $m$ is unique and is cyclic.

**3.** Let $F$ be a finite field. Prove that its characteristic $p$ is a prime number, that the number of elements of $F$ is $p^r$ with some integer $r \geq 1$, and that any subfield of $F$ has a number of elements of the form $p^s$ where $s$ divides $r$. Prove also that, conversely, for any divisor $s$ of $r$ there is a unique subfield of $F$ with $p^s$ elements.

**4.** What is the degree of the stem field of the polynomials $X^2+1$ and $X^2-X+1$
• over $\mathbb{Q}$ ?
• over $\mathbb{F}_p$ for $p = 2, 3, 5, 7$ ? For $p$ any prime?
`Hint:` for which value of $p$ does the multiplicative group $\mathbb{F}_p^\times$ contain a subgroup of order 4? of order 6?

**5.** **(a)** Prove that the polynomial $X^4+1$ is irreducible over $\mathbb{Q}$.
**(b)** Let $F_q$ be a finite field with $q$ elements. Prove that $X^4+1$ splits in $F_q$ into linear factors if and only if $q$ is congruent to 1 modulo 8.
`Hint`: $X^8 - 1 = (X^4+1)(X^4-1)$.
**(c)** Check that for any prime $p$, the polynomial $X^4+1$ is reducible over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
`Hint`: for any odd integer $a$, the number $a^2$ is congruent to 1 modulo 8.

**6.** Let $\sigma : F_1 \to F_2$ be a homomorphism of fields. Show that the two fields $F_1$ and $F_2$ have the same characteristic, hence the same prime field $F$. Show that $\sigma$ is a $F$–homomorphism.

**7.** Let $E$ be a field, $F$ a subfield of $E$, $\alpha_1$ and $\alpha_2$ two elements in $E$.
**(a)** Assume that there exists a $F$–homomorphism $\sigma : F(\alpha_1) \to F(\alpha_2)$ such that $\sigma(\alpha_1) = \alpha_2$. Prove that $\alpha_1$ is algebraic over $F$ if and only if $\alpha_2$ is algebraic over $F$.
**(b)** Assume $\alpha_1$ and $\alpha_2$ are transcendental over $F$. Prove that there exists a unique $F$–homomorphism $\sigma : F(\alpha_1) \to F(\alpha_2)$ such that $\sigma(\alpha_1) = \alpha_2$ and that $\sigma$ is an isomorphism.
**(c)** Assume $\alpha_1$ and $\alpha_2$ are algebraic over $F$. Prove that the following conditions are equivalent.
(i) $\alpha_1$ and $\alpha_2$ have the same irreducible polynomial over $F$.
(ii) There exists a $F$–homomorphism $\sigma : F(\alpha_1) \to F(\alpha_2)$ such that $\sigma(\alpha_1) = \alpha_2$.
If $\sigma$ exists, then it is unique and is an isomorphism.

**8.** Let $E$ be a field, $F$ a subfield of $E$, $\alpha$ and $\beta$ two elements in $E$ algebraic over $F$ of degrees $m$ and $n$ respectively. Assume $\gcd(m, n) = 1$. Prove that the field $F(\alpha, \beta)$ is a finite extension of $F$ of degree $mn$.

**9.** Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ be the finite field with 2 elements, $E = \mathbb{F}_2(T_1, T_2)$ the field of rational fractions in two variables over $\mathbb{F}_2$, $F$ the subfield $\mathbb{F}_2(T_1^2, T_2^2)$.
**(a)** Check that any $\gamma \in E$ satisfies $\gamma^2 \in F$.
**(b)** Show that $E/F$ is a finite extension and compute $[E : F]$.
`Hint.` Compute $[E : \mathbb{F}_2(T_1^2, T_2)]$ and $[\mathbb{F}_2(T_1^2, T_2) : F]$.
**(c)** Deduce that the finite extension $E/F$ is not simple.