NAP 2017. Module 4. Homework 2 Friday, July 14, 2017.

These excercises are due July 21, 2017, at 10 pm. Nepal time. Please, send them to nap@rnta.eu, to laurageatti@gmail.com and schoof.rene@gmail.com. Contact us if you have any question!

1. Let p be a prime and let f be an irreducible degree n polynomial in $\mathbf{F}_p[X]$. Show that the Galois group of f is contained in the alternating group A_n if and only if n is odd.

2. Let H be a transitive subgroup of the symmetric group S_n. Suppose that H contains a 2-cycle and an $(n-1)$-cycle. Show that $H = S_n$. (See Milne Lemma 4.32)

3. Determine the Galois groups over $\mathbf{Q}$ of the polynomials (they are all irreducible)
$$x^4 - 10x^2 + 1, \qquad x^4 - 8x^2 + 3, \qquad x^4 - 2x^2 + 25.$$

4. Let $f = x^5 - x + 3 \in \mathbf{Z}[X]$. This is an irreducible polynomial.
   (a) Show that f has three linear factors modulo 3.
   (b) Show that f is irreducible modulo 5.
   (c) Show that the Galois group of f over $\mathbf{Q}$ is S_5.

5. Let $g = x^5 + 8x + 3 \in \mathbf{Z}[X]$. This is an irreducible polynomial.
   (a) Show that f has three linear factors modulo 3.
   (b) Show that f is the product of a linear polynomial and an irreducible polynomial of degree 4 modulo 2.
   (c) Show that the Galois group of f over $\mathbf{Q}$ is S_5.

6. Let K be a field. Show that the Galois group of $X^n - 1$ over F is commutative (Hint: without loss of generality one may assume that the characteristic of K does not divide n. Show that any automorphism σ of the splitting field K_f of $X^n - 1$ is determined by $\sigma(\zeta)$, where ζ is a primitive n-th root of unity in K_f).

7. *(Optional)* The Möbius function $\mu : \mathbf{N} \longrightarrow \{-1, 0, +1\}$ is defined by
$$\mu(n) = \begin{cases} (-1)^r; & \text{if } n \text{ is a product of } r \text{ distinct primes,} \\ 0; & \text{otherwise.} \end{cases}$$
   (a) Compute $\mu(10)$, $\mu(20)$ and $\mu(30)$.
   (b) Show that μ is multiplicative, i.e. show that $\mu(nm) = \mu(n)\mu(m)$ if $\gcd(n, m) = 1$.
   (c) Let $f(n) = \sum_{d|n} \mu(d)$. Here the summation runs over the positive divisors d of $n \in \mathbf{N}$. Show that f is also a multiplicative function.
   (d) (Möbius inversion) Suppose that the sequences a_n, b_n satisfy $a_n = \sum_{d|n} b_n$ for all $n \geq 1$. Show that $b_n = \sum_{d|n} \mu(\frac{n}{d}) a_d$

8. *(Optional)* Let p be a prime and let N_n denote the number of irreducible polynomials in $\mathbf{F}_p[X]$ of degree n.
   (b) Compute N_4 and N_6 for any finite field $\mathbf{F}_p$.
   (a) Show that $\sum_{d|n} dN_d = p^n$ for every $n \geq 1$.
   (b) Show that $N_n = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$. (Use previous exercise)