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.*

Sol.: The Galois group of the splitting field of f is a cyclic group of order n, generated by the Frobenius automorphism. It can be identified with the group $\langle (12\ldots n)\rangle$ in S_n. One has that $(12\ldots n)$ is even, and therefore contained in 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)*

$$x^4 - 10x^2 + 1, \qquad x^4 - 8x^2 + 3, \qquad x^4 - 2x^2 + 25.$$

Sol.: (a) Since $f(x) = x^4 - 10x^2 + 1$ irreducible over $\mathbf{Q}$, its Galois group is a transitive subgroup of S_4 and is contained in A_4 (one has $disc(f) = 147456 = (384)^2$, which is a square). Its resolvent cubic is $g(x) = x^3 + 10x^2 - 4x - 40 = (x-2)(x+2)(x+10)$ is completely reducible over $\mathbf{Q}$. By the classification, $G_f = V_4$.

Remarks. The resolvent cubic g is completely reducible over $\mathbf{Q}$: consequently $\mathbf{Q}_g = \mathbf{Q}$. On the other hand, to each of the three subgroups of V_4

$$H_1 = \langle 1, (12)(34)\rangle, \quad H_2 = \langle 1, (13)(24)\rangle, \quad H_3 = \langle 1, (14)(23)\rangle$$

there is associated an intermediate quadratic extension of $\mathbf{Q}$

$$\mathbf{Q} \subset \mathbf{Q}_f^{H_i} \subset \mathbf{Q}_f, \qquad i = 1, 2, 3.$$

Denote by

$$\alpha_1 = \sqrt{5+2\sqrt{6}}, \quad \alpha_2 = -\sqrt{5+2\sqrt{6}}, \quad \alpha_3 = \sqrt{5-2\sqrt{6}}, \quad \alpha_4 = -\sqrt{5-2\sqrt{6}}$$

the four roots of f and by

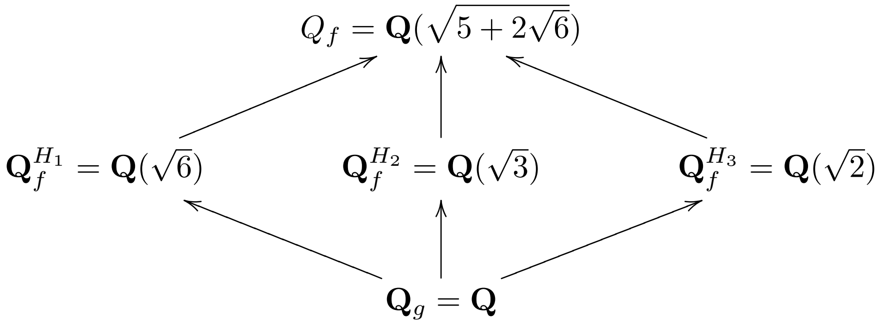
$$\alpha := \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \beta := \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \gamma := \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

the roots of g.

Consider $\mathbf{Q}(\alpha_1\alpha_2) = \mathbf{Q}(\sqrt{6})$. This is clearly an H_1-invariant quadratic extension of $\mathbf{Q}$, contained in $\mathbf{Q}_f = \mathbf{Q}(\sqrt{5+2\sqrt{6}}, \sqrt{5-2\sqrt{6}})$. More precisely, $\mathbf{Q}_f = \mathbf{Q}(\sqrt{5+2\sqrt{6}})$, since $(5+2\sqrt{6})(5-2\sqrt{6}) = 1$, which is a square in $\mathbf{Q}$ and therefore in $\mathbf{Q}(\sqrt{6})$.

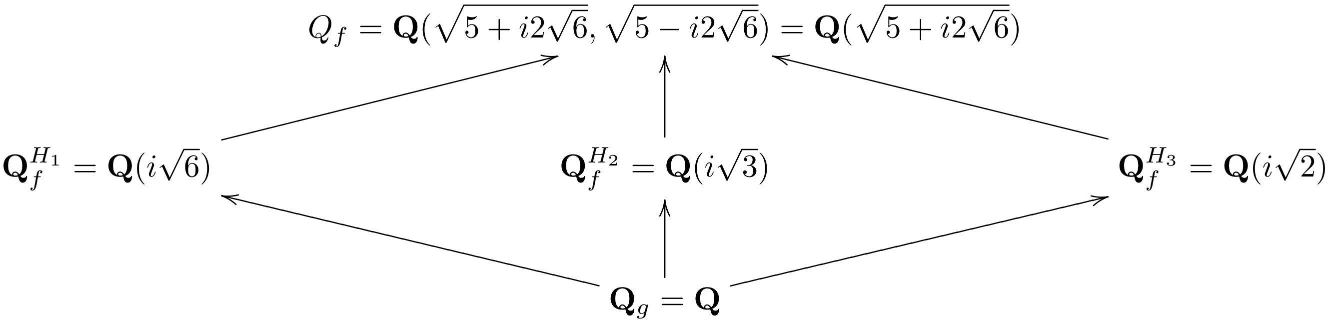
Next consider the quantities $(\alpha_1+\alpha_3)$ and $(\alpha_2+\alpha_4)$, which are H_2-invariant and satisfy the degree two equation $Y^2+(\alpha+\gamma) = Y^2-12 = 0$. This means that $\mathbf{Q}(\sqrt{3})$ is an H_2-invariant quadratic extension of $\mathbf{Q}$, contained in $Q_f = \mathbf{Q}(\sqrt{5+2\sqrt{6}})$ (note that $(5+2\sqrt{6})(5-2\sqrt{6}) = 1$, which is a square in $\mathbf{Q}$, is also a square in $\mathbf{Q}(\sqrt{3})$).

Finally consider the quantities $(\alpha_1+\alpha_4)$ and $(\alpha_2+\alpha_3)$, which are H_3-invariant and satisfy the degree two equation $Y^2+(\alpha+\beta) = Y^2-8 = 0$. This means that $\mathbf{Q}(\sqrt{2})$ is an H_3-invariant quadratic extension of $\mathbf{Q}$, contained in $Q_f = \mathbf{Q}(\sqrt{5+2\sqrt{6}})$ (note that $(5+2\sqrt{6})(5-2\sqrt{6}) = 1$, which is a square in $\mathbf{Q}$, is also a square in $\mathbf{Q}(\sqrt{2})$).



(c) The discriminant of $f(x) = x^4-2x^2+25$ is equal to $3686400 = (1920)^2$, hence G_f is a transitive subgroup of S_4, contained in A_4. The resolvent cubic of f is $g(x) = x^3+2x^2-100x-200 = (x+10)(x-10)(x+2)$, which is completely reducible over $\mathbf{Q}$. By the classification, $G_f = A_4$.

As in the previous case we have a diagram as follows:



(b) The discriminant of $f(x) = x^4-8x^2+3$ is equal to 129792, which is not a square. Hence G_f is a transtive subgroup of S_4, not contained in A_4. Its resolvent cubic is $g(x) = x^3+8x^2-12x-96 = (x+8)(x^2-12)$. In this case we have to decide whether $G_f \cong C_4$ or $G_f \cong D_4$; equivalently whether the degree $[\mathbf{Q}_f : \mathbf{Q}_g]$ is 2 or 4.

Denote by

$$\alpha_1 = \sqrt{4+\sqrt{13}}, \quad \alpha_2 = -\sqrt{4+\sqrt{13}}, \quad \alpha_3 = \sqrt{4-\sqrt{13}}, \quad \alpha_4 = -\sqrt{4-\sqrt{13}}$$

the four roots of f and by

$$\alpha := \alpha_1\alpha_2+\alpha_3\alpha_4 = -8, \quad \beta := \alpha_1\alpha_3+\alpha_2\alpha_4 = 2\sqrt{3}, \quad \gamma := \alpha_1\alpha_4+\alpha_2\alpha_3 = -2\sqrt{3},$$

the roots of g.

We have $\mathbf{Q}_f = \mathbf{Q}(\sqrt{4+\sqrt{13}}, \sqrt{4-\sqrt{13}})$ and $\mathbf{Q}_g = \mathbf{Q}(\sqrt{3})$.
The fields $\mathbf{Q}((\alpha_1+\alpha_3),(\alpha_2+\alpha_4))$ and $\mathbf{Q}((\alpha_1+\alpha_4),(\alpha_2+\alpha_3))$ are intermediate extensions: they are between $\mathbf{Q}_g$ and $\mathbf{Q}_f$. One computes that $\mathbf{Q}((\alpha_1+\alpha_3),(\alpha_2+\alpha_4)) = \mathbf{Q}(\sqrt{8+2\sqrt{3}})$ and $\mathbf{Q}((\alpha_1+\alpha_4),(\alpha_2+\alpha_3)) = \mathbf{Q}(\sqrt{8-2\sqrt{3}})$. The numbers $8 \pm 2\sqrt{3}$ are not squares in $\mathbf{Q}(\sqrt{3})$, because their norms are equal to 52, which is not a square in $\mathbf{Q}$. This shows that both fields are degree 2 extensions of $\mathbf{Q}(\sqrt{3})$. To see that they are *distinct*, we observe that the product $(8+2\sqrt{3})(8-2\sqrt{3}) = 52$ is not a square in $\mathbf{Q}(\sqrt{3})$ either. Indeed, the equation $(x+y\sqrt{3})^2 = 52$ has no solutions $x, y \in \mathbf{Q}$. This proves that G_f cannot be isomorphic to C_4, but it is necessarily isomorphic to D_4.

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.

Sol.: (a) In $\mathbf{F}_3[x]$, the polynomial becomes

$$f(x) = x^5 - x = x(x-1)(x+1)(x^2+1),$$

where x^2+1 is an irreducible factor.

(b) In $\mathbf{F}_5[x]$ the polynomial f is irreducible: it has no linear factors, nor degree 2 factors....

(c) By (a) and (b), the Galois group G_f of f over $\mathbf{Q}$ contains a 2-cycle and a 5-cycle. Now Lemma 4.32 in [Milne] ensures that $G_f \cong S_5$.

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.

Sol.: (a) In $\mathbf{F}_3[x]$ the polynomial g becomes $g(x) = x^5 - x = x(x-1)(x+1)(x^2+1)$, where x^2+1 is an irreducible factor.

(b) In $\mathbf{F}_2[x]$ the polynomial g becomes $g(x) = x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$. The degree 4 factor is irreducible because 2 is a primitive root in $\mathbf{F}_5$ (cf. Excercises 1, n.6).

(c) By (a) and (b), the Galois group G_f of f over $\mathbf{Q}$ contains a 2-cycle and a 4-cycle. Now Lemma 4.32 in [Milne] ensures that $G_f \cong S_5$.

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

Sol.: Assume that $char(K) = p$, with p prime and that $n = mp^r$, with $\gcd(p, m) = 1$. Then $X^n - 1 = X^{mp^r} - 1 = (X^m - 1)^{p^r}$. This means that the splitting field of $X^n - 1$ is the same as the splitting field of $f(X) = X^m - 1$. Hence, without loss of generality we may assume that the characteristic of $\mathbf{K}$ does not divide n. The roots of f form a finite and hence cyclic subgroup of $\mathbf{K}^*$. So they are $\xi, \xi^2, \ldots, \xi^m = 1$, where ξ is a generator. Hence $\mathbf{K}_f = \mathbf{K}(\xi)$. Any automorphism $\sigma \in Aut(\mathbf{K}_f/\mathbf{K})$ is determined by $\sigma(\xi)$ (being an automoprhism implies $\sigma(\xi^k) = \sigma(\xi)^k$) and must be of the form $\sigma(\xi) = \xi^r$, for some $r \in \mathbf{Z}$. Since also ξ^r must be a primitive root of 1, then $\gcd(r, m) = 1$. It follows that the map that sends σ to r is a well defined group homomorphism $\psi : G_f \longrightarrow \mathbf{Z}_n^*$ Since ψ is injective, it follows that G_f is abelian.

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* $a_n = \sum_{d|n} b_d$ *for all* $n \geq 1$. *Show that* $b_n = \sum_{d|n} \mu(\frac{n}{d}) a_d$

Sol.: (a) $10 = 2 \cdot 5$ and $\mu(10) = (-1)^2 = 1$;
$20 = 2^2 \cdot 5$ and $\mu(20) = 0$;
$30 = 2 \cdot 3 \cdot 5$ and $\mu(30) = (-1)^3 = -1$.
(b) If either n or m contains a square, then so does nm and $\mu(nm) = 0 = \mu(n)\mu(m)$. If both n and m are square free, then nm is square free if and only if $gcd(n, m) = 1$. In this case the prime factors of nm are the disjoint union of the prime factors of n and those of m, implying that $\mu(nm) = \mu(n)\mu(m)$.
(c) If $\gcd(n, m) = 1$, then the divisors d of nm are of the form $d_1 d_2$, where d_1 is a divisor of n and d_2 is a divisor of m, and $\gcd(d_1, d_2) = 1$. Then, from $\mu(d_1 d_2) = \mu(d_1)\mu(d_2)$, we obtain

$$f(nm) = \sum_{d|nm} \mu(d) = \sum_{\substack{d_1 d_2 | nm \\ d_1|n,\ d_2|m}} \mu(d_1 d_2) = \sum_{d_1|n} \mu(d_1) \sum_{d_2|m} \mu(d_2).$$

(d) We evaluate $\sum_{d|n} \mu(\frac{n}{d}) a_d$. It is equal to

$$\sum_{d|n} \mu(\frac{n}{d}) \sum_{e|d} b_e.$$

Changing the order of summation we get

$$\sum_{e|n} \sum_{e|d|n} \mu(\frac{n}{d}) b_e.$$

In the second sum, d runs over the multiples of e that divide n. Writing $d' = d/e$, this becomes a sum over the divisors d' of n/e. We get

$$\sum_{e|n} \left(\sum_{d' | \frac{n}{e}} \mu(\frac{n/e}{d'}) \right) b_e.$$

Since $\sum_{d|m} \mu(\frac{n}{d}) = \sum_{d|m} \mu(d)$ is equal to 1 for $m = 1$ and zero otherwise, we wee that the second sum only gives a non-zero contribution for $e = n$. In other words, the sum is equal to b_n as required.

(By part (c) it suffices to check that $\sum_{d|m} \mu(d)$ is zero, for $m > 1$ a power of a prime)

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.*
   (a) Compute N_4 and N_6 for any finite field $\mathbf{F}_p$.
   (b) Show that $\sum_{d|n} dN_d = p^n$ for every $n \geq 1$.
   (c) Show that $N_n = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$. (Use previous exercise)

Sol.: We can count irreducible polynomials of degree n in $\mathbf{F}_p[X]$ by counting the elements of $\mathbf{F}_{p^n}$ whose minimum polynomial has degree n and dividing the result by n (every such polynomial has n zeros in $\mathbf{F}_{p^n}$). Recall that the elements of $\mathbf{F}_{p^n}$ whose minimum polynomial has degree less than n are those lying in proper subfields of $\mathbf{F}_{p^n}$, namely in fields $\mathbf{F}_{p^d}$, with $d|n$.

(a)

$$N_4 = \frac{1}{4}(\#\mathbf{F}_{p^4} - \#\mathbf{F}_{p^2}) = \frac{1}{4}(p^4 - p^2);$$

$$N_6 = \frac{1}{6}(\#\mathbf{F}_{p^6} - \#\mathbf{F}_{p^2} - \#\mathbf{F}_{p^3} + \#\mathbf{F}_p) = \frac{1}{6}(p^6 - p^2 - p^3 + p);$$

(b) The elements of $\mathbf{F}_{p^n}$ can be subdivided according to the degree d of their minimum polynomial (necessarily a divisor of n). The number of elements in $\mathbf{F}_{p^n}$ whose minimum polynomial has degree d is d times the number of irreducible polynomials of degree d in $\mathbf{F}_p[X]$. Hence

$$p^n = \sum_{d|n} dN(d).$$

(c) Let $a_n = p^n$ and $b_n = nN(n)$. By part (b) we have $a_n = \sum_{d|n} b_d$ and hence by the previous exercice $b_n = \sum_{d|n} \mu(\frac{n}{d}) a_d$.