These excercises are due July 12, 2017, at 10 pm. Nepal time. Please, send them to nap@rnta.eu and to laurageatti@gmail.com and schoof.rene@gmail.com. Contact us if you have any question!

1. *Let p be a prime. Prove that there are infinitely many irreducible polynomials in $\mathbf{F}_p[x]$.*

Sol.: For every $n \in \mathbf{N}$, there is a finite field with p^n elements which can be obtained as the splitting field of an irreducible polynomial in $\mathbf{F}_p$ of degree n. Hence there are infinitely many irreducible polynomials in $\mathbf{F}_p[x]$.

2. (a) *Prove that the Frobenius automorphism of $\mathbf{F}_5[\sqrt{2}]$ sends $\sqrt{2}$ to $-\sqrt{2}$.*
   (b) Compute the order of $1-\sqrt{2},\ 2-\sqrt{2},\ 3-\sqrt{2}$ in $\mathbf{F}_5[\sqrt{2}]^*$.

Sol.: (a) Set $\alpha := \sqrt{2}$. Then α is a zero of the irreducible quadratic polynomial $x^2 - 2 \in \mathbf{F}_5[x]$. Therefore it satisfies $\alpha^2 = 2$. Let $\phi(x) = x^5$ be the Frobenius automorphism. Then

$$\phi(\alpha) = \alpha^5 = \alpha^2\alpha^2\alpha = 4\alpha = -\alpha.$$

(b) Recall that $\mathbf{F}_5[\sqrt{2}]^*$ is a cyclic group of order $24 = 2^3 \cdot 3$, and the order of an element in $\mathbf{F}_5[\sqrt{2}]^*$ has to be a divisor of 24, i.e $1, 2, 4, 8, 6, 12, 24$.
Moreover by (a), one has $N(\alpha) = \alpha\phi(\alpha) = -\alpha^2 = -2$.

Now we can start computing the powers of our elements.

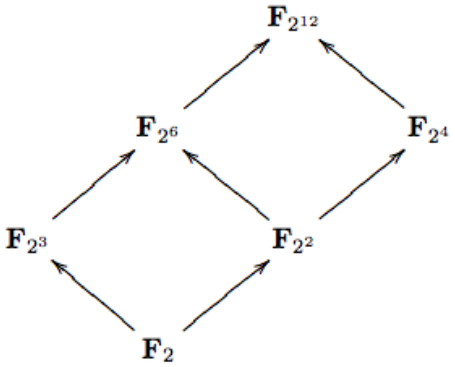
• $(1-\alpha)$
$(1-\alpha)^2 = 1 + 2 - 2\alpha = 3 + 3\alpha, \quad (1-\alpha)^3 = (1-\alpha)(3+3\alpha) = 3 + 3\alpha - 3\alpha - 3\alpha^2 = 3 - 6 = 2,$
At this point it is clear that the order of $(1-\alpha)$ is not 4, because $(1-\alpha)^2 = 2 - 2\alpha$, and it is not 8, because $(1-\alpha)^8 = (2-2\alpha)^2 \neq 1$.

$$(1-\alpha)^3 \cdot (1-\alpha)^3 = (1-\alpha)^6 = 4 = -1, \qquad (1-\alpha)^6(1-\alpha)^6 = (1-\alpha)^{12} = 1.$$

Conclusion: $(1-\alpha)$ has order 12.
The orders of $(2-\alpha)$ and $(3-\alpha)$ can be computed in a similar way.

3. *How many proper subfields does $\mathbf{F}_{2^{12}}$ have? Explain...*

Sol.: The proper subfields $\mathbf{F}_{2^{12}}$ are in one-to-one corresponedence with the proper divisors of 12, which are 1, 2, 3, 4, 6. The diagram of the inclusions is the following



4. *Is the polynomial x^2+x+1 irreducible or not in $\mathbf{F}_2[x]$? and in $\mathbf{F}_4[x]$?*

Sol.: The polynomial $f(x)=x^2+x+1$ irreducible in $\mathbf{F}_2[x]$, because $f(0)=f(1)=1\neq 0$. Since $\mathbf{F}_4$ is the splitting field of every irreducible polynomial of degree 2 in $\mathbf{F}_2[x]$, the polynomial f factors in $\mathbf{F}_4[x]$.

5. *Given the polynomial x^3+2 in $\mathbf{F}_5[x]$, compute the order of its roots in the multipicative group of its splitting field.*

Sol.: One can easily see that $x^3+2=(x-2)(x^2-2x-1)$ in $\mathbf{F}_5[x]$ and that x^2-2x-1 is irreducible. Hence the splitting field of x^3+2 is a quadratic extension of $\mathbf{F}_5$, namely $\mathbf{F}_{25}\cong\mathbf{F}_5[x]/(x^2-2x-1)$. The order of $\alpha=2$ in $\mathbf{F}_{25}^*$ is just the order of 2 in $\mathbf{F}_5^*$ and it is equal to 4.
If α is any of the roots of x^2-2x-1, we compute its powers using the relation $x^2=2x+1$ and keeping in mind that the order of an element in $\mathbf{F}_{25}^*$ can be 1,2,3,4,6,8,12,24.

$$\alpha^2=2\alpha+1,\quad \alpha^3=\alpha(2\alpha+1)=2\alpha^2+\alpha=2,\quad \alpha^4=2\alpha,\quad \alpha^5=4\alpha+2,\quad \alpha^6=\alpha(4\alpha+2)=4=-1.$$

At this point it is clear that α has order 12

$$\alpha^{12}=(\alpha^6)^2=1.$$

6. *Give an explicit isomorphism $\mathbf{F}_5[x]/(x^2+x+1)\to\mathbf{F}_5[\sqrt{2}]$.*

Sol.: Both fields are quadratic extensions of $\mathbf{F}_5$, so they are isomorphic. A field homomorphism is necessarily injective, and in our case also surjective. It is completely determined by $\phi(1)=1$ and $\phi(x)$. But to have a homomorphism, we must make sure that the ideal (x^2+x+1) lies in the kernel of ϕ. In other words $\phi(x)=a+b\sqrt{2}$ must be an element of $\mathbf{F}_5[\sqrt{2}]$ which satisfies the equation $(a+b\sqrt{2})^2+(a+b\sqrt{2})+1=0$. This leads to the system modulo 5

$$\begin{cases} a^2+2b^2+a+1=0 \\ b(2a+1)=0 \end{cases} \quad\Leftrightarrow\quad \begin{cases} a=2 \\ b=2,3. \end{cases}$$

So we have two choices for ϕ

$$\phi(x)=2+2\sqrt{2}\qquad\text{and}\qquad \phi(x)=2+3\sqrt{2}.$$

7. (a) *What is the degree of the smallest field extension of $\mathbf{F}_5$ which contains an element of multiplicative order 13.*
   (b) Determine the degrees of the irreducible factors of $x^{13}-1$ in $\mathbf{F}_5[x]$.

Sol.: (a) The degree of the smallest field extension of $\mathbf{F}_5$ which contains an element of multiplicative order 13 is the smallest positive integer k for which $\#\mathbf{F}_{5^k}^*=5^k-1$ is divisible by 13. This is a necessary condition, and it is also sufficient because $\mathbf{F}_{5^k}^*$ is a cyclic group and contains elements of order d, for every d dividing its order. The smallest such k is 4.
(b) Write

$$x^{13}-1=(x-1)\frac{x^{13}-1}{x-1}.$$

The degree 12 polynomial $\frac{x^{13}-1}{x-1}$ is irreducible in $\mathbf{F}_5[x]$ if and only if 5 is a primitive root in $\mathbf{Z}_{13}^*$, if and only if it has order 12. We have

$$5, \quad 5^2 \equiv -1, \quad 5^3 \equiv -5, \quad 5^4 \equiv 1 \mod 13.$$

Then 5 has order 4 in $\mathbf{Z}_{13}^*$ and $\frac{x^{13}-1}{x-1}$ is not irreducible in $\mathbf{F}_5[x]$.

We claim that it splits into the product of 3 irreducible factors of degree 4, equal to the order of 5 in $\mathbf{Z}_{13}^*$. Let m be the degree of an irreducible factor g and let ζ be a zero of g. Then m is the smallest integer d for which $\zeta \in \mathbf{F}_{5^d}$, and $\zeta^{5^d-1} = 1$ (by Fermat thm.). On the other hand $\zeta^{13} = 1$ and ζ has order 13. Consequently

$$13 \mid 5^m - 1 \quad \Leftrightarrow \quad 5^m \equiv 1 \bmod 13,$$

and m is the smallest integer with this property. This means that m is the order of 5 in $\mathbf{Z}_{13}^*$ and is the same for all irreducible factors of $\frac{x^{13}-1}{x-1}$ in $\mathbf{F}_5[x]$. In this case there are 3 of them.

8. *Compute the discriminant of the polynomial* $x^7 + x + 1 \in \mathbf{Z}[x]$.

Sol.: To illustrate the algorithm we compute the discriminat of the polynomial $f(x) = x^n + x + 1$, following the note on resultants:

$$disc(f) = (-1)^{\frac{n(n-1)}{2}} Res(f, f') = (-1)^{\frac{n(n-1)}{2}} Res(f', f) =$$

$$= (-1)^{\frac{n(n-1)}{2}} (-1)^{n(n-1)} Res(nx^{n-1} + 1, x^n + x + 1) = (-1)^{\frac{n(n-1)}{2}} Res(nx^{n-1} + 1, x^n + x + 1).$$

Write $f = qf' + r$, with $r(x) = \frac{n-1}{n}x - 1$. Then

$$disc(f) = (-1)^{\frac{n(n-1)}{2}} n^{n-1} Res(nx^{n-1} + 1, \tfrac{n-1}{n}x - 1) =$$

$$= (-1)^{\frac{n(n-1)}{2}} n^{n-1} (-1)^{n-1} Res(\tfrac{n-1}{n}x - 1, nx^{n-1} + 1) =$$

$$= (-1)^{\frac{3n(n-1)}{2}} n^{n-1} (\tfrac{n-1}{n})^{n-1} \left(n(\tfrac{n}{n-1})^{n-1} + 1 \right) =$$

$$= (-1)^{\frac{n(n-1)}{2}} (n-1)^{n-1} \left(n(\tfrac{n}{n-1})^{n-1} + 1 \right) =$$

$$= (-1)^{\frac{n(n-1)}{2}} \left(n^n + (n-1)^{n-1} \right).$$

For $n = 7$ we get

$$-(7^7 + 6^6) = -870199.$$

9. *Let* $f = x^2 + x + 1$ *in* $\mathbf{F}_2[x]$. *Show that its Galois group* G_f *is not contained in* $A_2 = \{Id\}$, *despite the fact that its discriminant is a square in* $\mathbf{F}_2$.

Sol.: The polynomial f is irreducible over $\mathbf{Q}$; consequently it has distinct zeros α and β. The Galois group G_f is non-trivial (hence $\neq A_2$), since it contains the non-trivial element which switches α and β. Every element in $\mathbf{F}_2$ is a square, so $disc(f)$ being a square puts no restriction.

10. *Exhibit a transitive subgroup of* S_4 *different from* A_4 *and* S_4.

Sol.: One example is the group of cyclic permutations of $\{1, 2, 3, 4\}$, generated by (1234); another one is the group generated by the elements (1234) and (14)(23), isomorphic to D_4.