

**These exercises are due July 12, 2017, at 10 pm. Nepal time. Please, send them to [nap@rnta.eu](mailto:nap@rnta.eu) and to [laurageatti@gmail.com](mailto:laurageatti@gmail.com) and [schoof.rene@gmail.com](mailto: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  $\mathbf{F}_p[x]$ .
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  $\mathbf{F}_5[\sqrt{2}]^*$ .
3. How many proper subfields does  $\mathbf{F}_{2^{12}}$  have? Explain...
4. Is the polynomial  $x^2 + x + 1$  irreducible or not in  $\mathbf{F}_2[x]$ ? and 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 multiplicative group of its splitting field.
6. Give an explicit isomorphism  $\mathbf{F}_5[x]/(x^2 + x + 1) \rightarrow \mathbf{F}_5[\sqrt{2}]$ .
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  $\mathbf{F}_5[x]$ .
8. Compute the discriminant of the polynomial  $x^7 + x + 1 \in \mathbf{Z}[x]$ .  
*Note: Question number 8 is optional.*
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  $\mathbf{F}_2$ .
10. Exhibit a transitive subgroup of  $S_4$  different from  $A_4$  and  $S_4$ .