Problem List 4

Weronika Jakimowicz

sometime in the future

Exercise 1. Calculate cyclotomic polynomials

$$F_1(X), F_2(X), F_4(X), F_8(X), F_{16}(X), F_{15}(X)$$

and then calculate their images in the ring $\mathbb{Z}_3[X]$, under the homomorphism $\mathbb{Z}[X] \to \mathbb{Z}_3[X]$ induced by the quotient homomorphism $\mathbb{Z} \mapsto \mathbb{Z}_3$. Which of them are irreducible over $\mathbb{Z}_3$?

$F_1(X) = X - 1$ is easy, then $X^2 - 1 = (X-1)(X+1)$, so $F_2(x) = x + 1$ because $x = 1$ is not a primitive root of order 2.

With $F_4(X)$ I know that it cannot have degree 4 because 2 divides 4 and cannot be counted in $\phi(4)$. I use the definition of F_m from the lecture and write:

$$\begin{aligned} F_4(x) &= (x - e^{\frac{\pi i}{2}})(x - e^{\frac{3\pi i}{2}}) = x^2 - x(e^{\frac{3\pi i}{2}} + e^{\frac{\pi i}{2}}) + e^{2\pi i} = \\ &= x^2 + 1 \end{aligned}$$

However, I think I could get it from the fact that the roots of a cyclotomic polynomial F_m are all the primitive roots of 1 of order m. So

$$x^4 - 1 = (x^2 - 1)(x^2 + 1)$$

and every root that comes from $x^2 - 1$ is not primitive, so only $x^2 + 1$ has primitive roots of order 4.

A similar story is with F_8 :

$$x^8 - 1 = (x^4 - 1)(x^4 + 1) \implies F_8(x) = x^4 + 1$$

$F_{15}(x)$ should have degree 8 and so here is a lot of computation to avoid multiplying $\prod_{\substack{1 \leq k < 15 \\ \gcd(k,15)=1}} (x - e^{k\frac{2\pi i}{15}})$

because why not

$$\begin{aligned} x^{15} - 1 &= (x-1)(x^{14} + x^{13} + \ldots + x + 1) = \\ &= (x-1)(x^{12}(x^2+x+1) + x^9(x^2+x+1) + \ldots + x^2 + x + 1) = \\ &= (x-1)(x^2+x+1)(x^{12} + x^9 + x^6 + x^3 + 1) = \\ &= (x-1)(x^2+x+1)(x^{12} + x^{11} - x^{11} + x^{10} - x^{10} + \ldots + x^3 + x^2 - x^2 + x - x + 1) = \\ &= (x-1)(x^2+x+1)(x^8(x^4+x^3+x^2+x+1) - x^7(x^4+1) + x^6(x^4 + \ldots + 1) - \ldots + (x^4+x^3+x^2+x+1)) = \\ &= \underbrace{(x-1)}_{=F_1(x)}\underbrace{(x^2+x+1)}_{\text{div. } F_3(x)}\underbrace{(x^4+x^3+x^2+x+1)}_{\text{div. } F_5(x)}(x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1) \end{aligned}$$

$$\Downarrow$$

$$F_{15}(x) = x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

And now for the final boss because I messed up the order in which they should appear and am too lazy to change it: $F_{16}(x)$!!! I expect it to have order 8

$$x^{16} - 1 = (x^8 - 1)(x^8 + 1) \implies F_{16}(x) = x^8 + 1$$

Images in $\mathbb{Z}_3[X]$:

$$F_1(x) = x - 1 \mapsto x + 2$$
$$F_2(x) = x + 1 \mapsto x + 1$$
$$F_4(x) = x^2 + 1 \mapsto x^2 + 1$$
$$F_8(x) = x^4 + 1 \mapsto x^4 + 1$$
$$F_{16}(x) = x^8 + 1 \mapsto x^8 + 1$$
$$F_{15}(x) = x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \mapsto x^8 + 2x^7 + x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1$$

Let me start from $F_{15}(x)$. I see that 2 divides $F_{15}(x)$ and it is easy to check that $(x + 1)^8 = F_{15}(x)$ in $\mathbb{Z}_3$.

Now, $F_4(x)$, it has no roots in $\mathbb{Z}_3$ and because it is a quadratic polynomial, it cannot be divided by any other polynomial than one of degree 1. Hence, it is irreducible.

$F_8(x)$ also has no roots in $\mathbb{Z}_3$ so we surely cannot split it into a linear polynomial and a polynomial of degree 3. The only hope is in two polynomials of degree 2. Let us check

$$(x^2 + x + 2)(x^2 + 2x + 2) = x^4 + 2x^3 + 2x^2 + x^3 + 2x^2 + 2x + 2x^2 + x + 1 = x^4 + 1$$

$F_{16}(x)$ is the worst because I cannot find a decomposition using simple tricks but showing that it is irreducible can be a little painful. I will leave it for now and most probably forget to return to it later. I apologize.

Exercise 2. Describe the normal closures of the following field extensions:

(a) $\mathbb{Q}[\sqrt[n]{2}] \supseteq \mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[n]{X}) \supseteq \mathbb{Q}(X)$

(c) $\mathbb{C}(\sqrt[n]{X}) \supseteq \mathbb{C}(X)$

(d) $\mathbb{Q}[\zeta] \supseteq \mathbb{Q}$, where ζ is a primitive root of 1 of degree $n > 1$.

(hint: in (a)–(c) find the minimal polynomial, in (c) use the fact that $\mathbb{C}$ is algebraically closed, in (b) notice that X may be replaced by any transcendental number, this is not necessary, but it helps.)

(a) $\mathbb{Q}[\sqrt[n]{2}] \supseteq \mathbb{Q}$

The minimal polynomial for $\sqrt[n]{2}$ over $\mathbb{Q}$ is $w(x) = x^n - 2$ and its roots are of form

$$a_k = \sqrt[n]{2}e^{\frac{2\pi i}{n}k}$$

Now, I know that an extension of a field is normal if for any polynomial, if it has one root, then it has all the roots. So I need to find the minimal field that contains all those roots and $\mathbb{Q}[\sqrt[n]{2}]$ and it is

$$L = \mathbb{Q}(a_1, ..., a_n = \sqrt[n]{2})$$

because we have already showed that it is the smallest field such that $a_1, ..., a_n$ are contained within it.

Exercise 3. Prove that every field extension of degree 2 is normal.

Let K be a field and $f \in K[X]$ be a polynomial of degree 2, WLOG f is monic. We consider K(a), where $f(a) = 0$. Let us assume that

$$f(x) = \alpha_0 + \alpha_1 x + x^2$$

for $\alpha_0, \alpha_1 \in K$. We know that if a, b are solutions of f, then $a + b = -\alpha_1 \implies b = -\alpha_1 - a \in K$, hence both roots of f are in our extension K(a) and K(a) is normal.