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 $\prod_{\substack{1 \le k < 15 \\ \gcd(k,15)=1}} (x - e^{k\frac{2\pi i}{15}})$

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.

Exercise 4. Assume that the field extension $K \subseteq L$ is algebraic and $f : L \to L$ is a monomorphism, $f \restriction K = id$. Prove that f is "onto".

Let us take any $\alpha \in L$ such that $\alpha \neq 0$. Then, since $K \subseteq L$ is algebraic, we know that there exists a minimal polynomial $w \in K[X]$ such that $w(\alpha) = 0$. Let

$$w(x) = \sum_{i=0}^{n} a_i x^i$$

and since w is minimal, then it is irreducible and $a_0 \neq 0$. Now, consider

$$f(w(\alpha)) = f(\sum a_i \alpha^i) = \sum f(a_i \alpha^i) = \sum f(a_i) f(\alpha^i) = \sum a_i \cdot f(\alpha)^i$$

Hence, $f(\alpha)$ must be another root of w. Since f is a monomorphism, we cannot have that two roots go to the same roots but we still need all of them to permute. Hence, every element of L is represented in Im(f).

Exercise 5. Show that if $K \subseteq L \subseteq \widehat{K}$ and $K \subseteq L$ is radical, then $Gal(\widehat{K}/K) = Gal(\widehat{K}/L)$.

$K \subseteq L$ is radical means that if $a \in L$ and $w_a \in K[X]$ is the minimal polynomial of a, then w_a has only one root in $\widehat{K}$

$$Gal(\widehat{K}/K) = Gal(\widehat{K}/L)$$

$\supseteq$ is obvious because $f \restriction L = id_L$ and $id_L \restriction K = id_K$ so $f \restriction K = id_K$.

$\subseteq$

Take any $f \in Gal(\widehat{K}/K)$ and any $a \in L$. I know that $w_a \in K[X]$ has only one root in $\widehat{K}$ and that this root is a. Let $w_a = \sum b_i x^i$ and see that

$$f(w_a(a)) = f(\sum b_i a^i) = \sum f(b_i) f(a^i) = \sum b_i f(a)^i = 0$$

so f(a) must also be a root of w_a and because this root is unique, then f(a) = a.

Exercise 7. Assume that char(K) = p > 0 and $a \in \widehat{K}$ is separable over K. Prove that $K(a) = K(a^p)$. (Hint: consider the minimal polynomial of a over K.)

Let $w_a \in K[X]$ be the minimal polynomial of a and because a is separable, then $w_a(x)$ has only simple roots in $\widehat{K}$. Furthermore, we cannot have $w_a(x) \in K[X^p]$.

Frobenius function $F(x) = x^p$ goes brrrr? I know that a^p is a root of $F(w_a(x))$ and that there exists a minimal n such that $[a^p]^n = a$. Hecne, $x^{pn} - x$ is a polynomial with derivative equal to -1 that assumes 0 at x = a. So, if I plug in a^p it also is zero and the derivative does not change. So the minimal polynomial of a^p must divide this badboy and because of this $w_{a^p} \notin K[X^p]$?

Exercise 8. (a) Prove that if $a \in L$ is radical over K, then $deg(a/K) = \min\{p^n : a^{p^n} \in K\}$

(b) Conclude that if a finite extension $K \subseteq L$ is radical, then its degree is a power of p (here p = char(K)).

(a) Ok, so $w_a(x)$, the minimal polynomial of a, has only one root in $\widehat{K}$.

I know that there exists aminimal n such that $a^{p^n} \in K$ and that $w_a(x)$ divides $x^{p^n} - a^{p^n}$. From this I get that $deg(a/K) \leq p^n$.

Now, let k = deg(a/K), then $w_a = (x-a)^k$ and using binomial something something

$$(x-a)^k = x^k - \binom{k}{1} x^{k-1} a + \dots + \binom{k}{k-1} x a^{k-1} + a^k \in K[X]$$

so firstly, k must be divisible by p for $\binom{k}{m} x^{k-m} a^m$ to disappear if $a \notin K$. Secondly, a^k must be the lowest power of a to be inside of K.

Exercise 9. Assume that $K \subseteq L, M \subseteq \widehat{K}$ are field extenstions such that $L \cap M = K$. Prove that if

$$(\forall\, K \subseteq_{fin} L_0 \subset L)(\forall\, K \subseteq_{fin} M_0 \subseteq M)\ [L_0(M_0) : L_0] = [M_0 : K],$$

then $[L(M) : L] = [M : K]$.

$$[M_0(L_0) : M_0][M_0 : K] = [M_0(L_0) : K] = [L_0(M_0) : K] = [L_0(M_0) : L_0][L_0 : K]$$

From the previous list I know that

$$[L(M) : L][L : K] = [L(M) : K] \leq [L : K][M : K]$$

and so

$$[L(M) : L] \leq [M : K].$$

So now I need the $\geq$ inequality.

$$\begin{aligned}[L(M) : K] = [L(M) : L_0(M_0)][L_0(M_0) : K] = [L(M) : L_0(M_0)][L_0(M_0) : L_0][L_0 : K] = \\ = [L(M) : L_0(M_0)][M_0 : K][L_0 : K] \geq [LM : L_0M_0][L_0M_0 : K] = [LM : K]\end{aligned}$$

which implies that in this case

$$[LM : K] = [L : K][M : K]$$

and so

$$[LM : K] = [LM : L][L : K]$$

$$[L(M) : K] = [L(M) : M][M : K]$$

$$[L(M) : K] = [L(M) : L_0(M_0)][M_0 : K]$$

$$\begin{aligned}[LM : K] = [LM : M][M : K] = [LM : M][M : M_0][M_0 : K] = [LM : M][M : M_0][L_0M_0 : L_0] \\ [LM : K] = [LM : L][L : L_0][L_0 : K]\end{aligned}$$

Exercise 11. Assume that the numbers $m, n > 1$ are relatively prime and $\zeta_n, \zeta_m \in \mathbb{C}$ are primitive roots of 1 of degree n, m respectively. Prove that $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. (Hint: notice that $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{mn})$. Rely on the fact that $\phi(mn) = \phi(m)\phi(n)$ for any co-prme m, n (without proof).)

Ok, so first I show that $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$.

$\subseteq$

$$\zeta_{nm} = e^{\frac{2\pi}{nm}}$$

$$\zeta_{nm}^n = e^{\frac{2n\pi}{nm}} = e^{\frac{2\pi}{m}} = \zeta_m$$

$$\zeta_{nm}^m = e^{\frac{2m\pi}{nm}} = e^{\frac{2\pi}{n}} = \zeta_n$$

$\supseteq$

$$\zeta_{nm} = e^{\frac{2\pi}{nm}} = e^{\frac{2a\pi}{m}} e^{\frac{2b\pi}{n}} = e^{\frac{2\pi(an+bm)}{mn}}$$

Now I have that

$$\phi(nm) = [\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = a \cdot \phi(n)$$

and if $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) \neq \mathbb{Q}$, then there is some power of ζ_n that is shared with ζ_m and so it would mean that $[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}(\zeta_n)] \neq \phi(m)$ which gives me a nice little contradiction.