Wielomiany cyklotomiczne

Karol Janowicz

November 2019

1 Wstęp

Wielomian $X^n - 1 \in \mathbb{Q}[X]$ ma n różnych pierwiastków w ciele liczb zespolonych $\mathbb{C}$, które tworzą grupę cykliczną o generatorze $\zeta = e^{\frac{2\pi i}{n}}$. Wynika stąd, że ciałem rozkładu tego wielomianu jest $\mathbb{Q}(\zeta)$. Ciało $\mathbb{Q}(\zeta)$ nazywa się często **ciałem cyklotomicznym**. Interesować nas będzie wielomian minimalny dla ζ zwany **wielomianem cyklotomicznym**. Za pomocą wielomianów cyklotomicznych udowodnimy także szczególny wariant twierdzenia Dirichleta mówiącego, że dla liczb względenie pierwszych $a, r \geq 1$, istnieje niskończenie wiele liczb pierwszych p o tej własności, że $p \equiv a \mod r$. My okażemy prawdziwość tego twierdzenia w przypadku, gdy $a = 1$ i $r > 1$ jest dowolną liczbą naturalną. Ogólnie, można rozważać rozszerzenie dowolnego ciała K o pierwiastek pierwotny z jedynki ζ; ciało $K(\zeta)$ nazywa się wtedy cyklotomicznym rozszerzeniem ciała K. Okazuje się, że każde takie rozszerzenie jest abelowe (i.e. jest Galois oraz jego grupa automorfizmów jest przemienna) i z tego powodu są bardzo ważne w algebrze.

2 Własności wielomianów cyklotomicznych

Definicja 2.1 (wielomian cyklotomiczny)**.** *Wielomianem cyklotomicznym (n-tym) nazywamy wielomian*

$$\Phi_n(X) = \prod_{\substack{1<k<n,\\(k,n)=1}} (X - e^{\frac{2\pi i k}{n}}) \in \mathbb{C}[X]$$

Zauważmy, że n-ty wielomian cyklotomiczny jest oczywiście stopnia $\varphi(n)$. Ponadto, wielomian Φ_n dzieli wielomian $X^n - 1$ i nie dzieli wielomianu $X^k - 1$, gdy $k < n$. Naszym celem jest okazanie, iż współczynniki wielomianu cyklotomicznego są całkowite oraz że jest on nierozkładalny nad $\mathbb{Q}$.

Lemat 2.1. $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Dowód. Wynika wprost z faktu, że każdy pierwiastek n-tego stopnia z 1 jest pierwiastkiem pierwotnym stopnia d, dla pewnego $d|n$, a także na odwrót. ■

Porównując ze sobą stopnie wielomianów występujących w powyższym lemacie, otrzymujemy znaną zależność: $n = \sum_{d|n} \varphi(d)$.

Przydatna w naszych rozważaniach okaże się **funkcja Möbiusa**.

Definicja 2.2. *Definiujemy funkcję Möbiusa* $\mu : \mathbb{N} \longrightarrow \{0, 1, -1\}$ *następująco:*

1. $\mu(1) = 1$
2. $\mu(n) = (-1)^k$, *gdy* n *jest iloczynem* k *różnych liczb pierwszych*
3. $\mu(n) = 0$, *gdy* n *jest kwadratowa, i.e. dzieli się przez kwadrat*

Odnotujmy natychmiast, że funkcja Möbiusa jest multiplikatywna, to znaczy $\mu(mn) = \mu(m)\mu(n)$, o ile $(n, m) = 1$. Zachodzi ponadto równość:

$$\sum_{d|n} \mu(d) = 0$$

dla każdego $n \neq 1$. Można ją też zapisać następująco

$$\sum_{\substack{n \\ d|n|m}} \mu\Big(\frac{m}{n}\Big) = 0$$

dla ustalonego $d|m$, gdzie $d < m$ (wystarczy napisać $m = dk$, $n = dl$). Możemy teraz udowodnić kluczowe

Twierdzenie 2.1 (wzór Möbiusa na odwrócenie)**.** *Niech* $f, g : \mathbb{N} \longrightarrow G$ *będą funkcjami o wartościach w grupie przemiennej* G *(z zapisem addytywnym). Przypuśćmy, że dla każdego* $n \in \mathbb{N}$ *zachodzi*

$$f(n) = \sum_{d|n} g(d)$$

Wtedy $g(n) = \sum_{d|n} \mu\big(\frac{n}{d}\big) f(d) = \sum_{d|n} f\big(\frac{n}{d}\big)\mu(d)$.

Dowód. Mamy

$$\sum_{d|n} \mu\big(\frac{n}{d}\big) f(d) = \sum_{d|n} \mu\big(\frac{n}{d}\big) \sum_{m|d} g(m) = \sum_{d|n} \sum_{m|d} \mu\big(\frac{n}{d}\big) g(m) = \sum_{m|n} g(m) \sum_{\substack{d, \\ m|d|n}} \mu\big(\frac{n}{d}\big)$$

W powyższej równości, ostatnia suma $\sum_{\substack{d, \\ m|d|n}} \mu\big(\frac{n}{d}\big)$ nie znika wtedy i tylko wtedy, gdy $m = n$. To dowodzi tezy. ■

Twierdzenie 1. ma liczne zastosowania. Odnotujmy dla przykładu, że skoro jest $n = \sum_{d|n} \varphi(d)$, to w związku ze wzorem na odwrócenie zachodzi równość

$$\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d) = n \sum_{d|n} \frac{\mu(d)}{d} = n\big(1 - \frac{1}{p_1}\big) \dots \big(1 - \frac{1}{p_m}\big)$$

gdzie $n = p_1^{k_1} \dots p_m^{k_m}$. My zaś chcemy wykorzystać lemat 1. i zastosować doń twierdzenie 1. Otrzymamy wtedy

Wniosek 2.1. *Dla każdego $n \in \mathbb{N}$ zachodzi równość*

$$\Phi_n(X) = \prod_{d|n} \big(X^d - 1\big)^{\mu(\frac{n}{d})}$$

Z powyższego wniosku możemy *explicite* wyznaczyć pierwsze kilka wielomianów cyklotomicznych: $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = \frac{X^3-1}{X-1} = X^2 + X + 1$, $\Phi_4(X) = \frac{X^4-1}{X^2-1} = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$. Ogólnie, dla liczby pierwszej p jest $\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + \dots + X + 1$. Stąd łatwo widać, że dla liczb pierwszych p, wielomiany cyklotomiczne Φ_p są rzeczywiście nierozkładalne (z kryterium Eisensteina).

Twierdzenie 2.2. *Wielomian cyklotomiczny $\Phi_n(X) \in \mathbb{C}[X]$ ma współczynniki całkowite.*

Dowód. Rozumujemy przez indukcję po n. Dla $n = 1$ sprawa jest jasna. Przypuśćmy, że teza jest prawdziwa dla wszysktich $k < n$. Rozważmy wielomian

$$\Phi(X) = \prod_{\substack{d|n,\\ d\neq n}} \Phi_d(X)$$

który ma współczynniki całkowite. Wiemy, że $X^n - 1 = \Phi(X)\Phi_n(X)$ nad $\mathbb{C}$. Ale, ponieważ $\Phi(X)$ jest moniczny, z twierdzenia o dzieleniu z resztą w pierścieniu $\mathbb{Z}[X]$ musi być $\Phi_n(X) \in \mathbb{Z}[X]$. ■

Powyższe twierdzenie można nieco wzmocnić, niczego nie modyfikując w dowodzie – można powiedzieć, że $\Phi_1(0) = -1$ oraz $\Phi_n(0) = 1$ dla $n > 1$. Twierdzenie 2. wynika także wprost ze wzoru Möbiusa na odwrócenie. Udowodnimy wreszcie

Twierdzenie 2.3. *Wielomian cyklotomiczny $\Phi_n(X) \in \mathbb{Z}[X]$ jest nierozkładalny nad ciałem $\mathbb{Q}$. W szczególności, rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ jest rozszerzeniem stopnia $\varphi(n)$, a ciało $\mathbb{Q}(\zeta)$ jest ciałem rozkładu wielomianu Φ_n.*

Zanim udowodnimy to twierdzenie, przyda nam się lemat.

Lemat 2.2. *Niech $g \in \mathbb{Z}[X]$ będzie nierozkładalnym dzielnikiem wielomianu Φ_n. Niech też ξ będzie pierwiastkiem g. Wówczas dla każdej liczby pierwszej p, względnie pierwszej z n, liczba ξ^p jest pierwiastkiem wielomianu g.*

Dowód. Napiszmy $\Phi_n(X) = g(X) \cdot h(X)$ dla pewnego $h \in \mathbb{Z}[X]$. Przypuśćmy, że dla pewnej liczby pierwszej p niedzielącej n, ξ^p nie jest pierwiastkiem g. Wtedy ξ^p jest pierwiastkiem $h(X)$ (bo ξ^p jest także pierwiastkiem pierwotnym stopnia n z jedynki). Mamy stąd, że ξ jest pierwiastkiem wielomianu $h(X^p)$, a więc $g(X)$ dzieli wielomian $h(X^p)$. Niech $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ oznacza rzut kanoniczny, zaś $\pi^* : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_p[X]$ indukowany homomorfizm pierścieni. Zauważmy, że $\pi^*\big(h(X^p)\big) = \pi^*\big(h(X)^p\big) = \pi^*\big(h(X)\big)^p$, toteż $\pi^*\big(g(X)\big)$ dzieli $\pi^*\big(h(X)\big)^p$. Niech więc $f(X) \in \mathbb{Z}_p[X]$ będzie nierozkładalnym dzielnikiem wielomianu $\pi^*\big(g(X)\big)$ (z tego, że wielomian $g(X) \in \mathbb{Z}[X]$ jest nierozkładalny nie wynika, że $\pi^*\big(g(X)\big)$ – także). Wtedy $f(X)$ dzieli $\pi^*\big(h(X)\big)^p$, a ponieważ pierścień $\mathbb{Z}_p[X]$ jest dziedziną z jednoznacznością rozkładu, to $f(X)$ dzieli $\pi^*\big(h(X)\big)$. Mamy stąd, że wielomian $f(X)^2$ dzieli $\pi^*\big(\Phi_n(X)\big) = \pi^*\big(g(X)\big) \cdot \pi^*\big(h(X)\big)$. To jest jednak niemożliwe, gdyż wielomian $\pi^*\big(X^n - 1\big)$ jest rozdzielczy nad ciałem $\mathbb{Z}_p$, ze względu na $(n, p) = 1$. ■

Użyteczność powyższego lematu wynika z faktu, że nierozkładalność wielomianu $f(X) \in \mathbb{Z}[X]$ implikuje nierozkładalność w pierścieniu $\mathbb{Q}[X]$. Jest to konsekwencja lematu Gaussa. Możemy teraz udowodnić twierdzenie 3.

Dowód twierdzenia 3. Niech $f \in \mathbb{Z}[X]$ będzie nierozkładalnym dzielnikiem wielomianu Φ_n, którego pierwiastkiem jest $\zeta = e^{\frac{2\pi i}{n}}$. Niech p będzie liczbą pierwszą względnie pierwszą z n. Z lematu ζ^p jest pierwiastkiem f. Stąd łatwo otrzymać, że **dla dowolnej** liczby naturalnej k względnie pierwszej z n, ζ^k jest pierwiastkiem f. Ale wszystkie pierwiastki pierwotne stopnia n są tej postaci, skąd natychmiast $f = \Phi_n$. Zatem Φ_n jest nierozkładalny nad $\mathbb{Z}$, skąd też nad $\mathbb{Q}$. ■

Odnotujmy ważną konksekwencję twierdzenia 3. Ciało cyklotomiczne $\mathbb{Q}(\zeta)$ jest izomorficzne z pierścieniem ilorazowym $\mathbb{Q}[X]/\big(\Phi_n(X)\big)$. Ponadto mamy homomorfizm grup $Gal\big((\mathbb{Q}(\zeta) : \mathbb{Q}\big) \longrightarrow \mathbb{Z}_n^*$, który automorfizmowi φ przyporządkowuje $\varphi(\zeta)$. To odzworowanie jest w istocie zanurzeniem – różnym automorfizmom odpowiadają różne wartości na pierwiastku ζ. Z równości rzędów (twierdzenie 3.) jest to w istocie izomorfizm grup! Jest to warte odnotowania, gdyż nie każde rozszerzenie cyklotomiczne indukuje izomorfizm jego grupy Galois z grupą $\mathbb{Z}_n^*$, a jedynie zanurzenie weń (np. wziąć $\mathbb{R} \subset \mathbb{C}$, które jest rozszerzeniem cyklotomicznym dla każdego n i jest stopnia 2).

Można udowodnić bardzo elegancki i piękny rezultat Kroneckera i Webera, że każde skończone, abelowe rozszerzenia ciała $\mathbb{Q}$ jest zawarte w pewnym jego rozszerzeniu cyklotomicznym.

3 Zastosowanie wielomianów cyklotomicznych

Udowodnimy wreszcie szczególny przypadek twierdzenia Dirichleta. Najpierw lemat.

Lemat 3.1. *Przypuśćmy, że liczba pierwsza p nie dzieli liczby naturalnej n. Wtedy*

$$\exists_{a\in\mathbb{Z}\setminus\{0\}}\ p \mid \Phi_n(a) \iff p \equiv 1 \mod n$$

Dowód. Zachodzi równość $X^n - 1 = \Phi_n(X)\prod_{\substack{d|n,\\ d<n}} \Phi_d(X)$ w pierścieniu $\mathbb{Z}[X]$. Popatrzmy na nią jak na równość w $\mathbb{Z}_p[X]$ (redukujemy współczynniki $\mod p$). Wtedy $p \mid \Phi_n(a)$ oznacza tyle, że a jest pierwiastkiem wielomianu $\Phi_n(X) \in \mathbb{Z}_p[X]$. Stąd natychmiast $a^n \equiv 1 \mod p$. W szczególności, rząd $a \in \mathbb{Z}_p^*$ dzieli n. Gdyby jednak $a^m \equiv 1 \mod p$ dla pewnego $m|n$, $m < n$, to wielomian $X^n - 1$ miałby pierwiastek wielokrotny w $\mathbb{Z}_p[X]$, co jest niemożliwe, bo $(n, p) = 1$. Zatem rząd a jest równy n. To zaś oznacza, że $n|p - 1$. W drugą stronę, niech $p \equiv 1 \mod n$. Wtedy w grupie cyklicznej $\mathbb{Z}_p^*$ istnieje element rzędu $n|p - 1$; oznaczmy go a. Wtedy $\Phi_n(a) = 0$ w $\mathbb{Z}_p$, a więc $p|\Phi_n(a)$. ■

Twierdzenie 3.1 (szczególny przypadek twierdzenia Dirichleta)**.** *Niech $n \in \mathbb{N}$, $n > 1$ będzie dowolną liczbą naturalną. Wtedy istnieje nieskończenie wiele liczb pierwszych czyniących zadość kongruencji $p \equiv 1 \mod n$.*

Dowód. Załóżmy, że dla pewnego $n > 1$ istnieje jedynie skończenie wiele liczb pierwszych $p_1, \ldots, p_k$ dających resztę 1 z dzielenia przez n. Z powyższego lematu wynika, że dla $a \in \mathbb{Z} \setminus \{0\}$, jedynymi dzielnikami pierwszymi liczby $\Phi_n(a)$, które nie dzielą liczby naturalnej n mogą być $p_1, \ldots, p_k$. Ale wstawiając $a = (np_1 \ldots p_k)^N$, mamy $\Phi_n(a) > 1$ dla odpowiednio dużego $N \in \mathbb{N}$; ponadto $\Phi_n(a) \equiv 1 \mod p_i$ dla $i = 1, \ldots, k$ oraz $\Phi_n(a) \equiv 1 \mod n$. Zatem $\Phi_n(a)$ ma inne dzielniki pierwsze niedzielące n poza $p_1, \ldots, p_k$, co jest absurdem. ■

Kolejny zastosowaniem wielomianów cyklotomicznych będzie twierdzenie Wedderburna, dotyczące skończonych pierścieni z dzieleniem.

Twierdzenie 3.2 (Wedderburna)**.** *Niech R będzie skończonym pierścieniem z dzieleniem (nie zakładamy przemienności!). Wówczas R jest ciałem.*

Dowód. Niech $q = |Z(R)|$ oznacza moc centrum pierścienia R, które w naszym wypadku jest ciałem. Pierścień R jest oczywiście przestrzenią wektorową nad $Z(R)$, skąd $|R| = q^n$. Zbiór $G = R \setminus \{0\}$ jest grupą ze względu na mnożenie. Możemy więc napisać równanie klas:

$$q^n - 1 = \sum |C(g)| = \sum \frac{q^n - 1}{|C_g|}$$

gdzie sumowanie odbywa się po wszystkich, parami rozłącznych klasach sprzężności w G (oznaczyliśmy je przez $C(g)$, a odpowiednie centralizatory przez C_g). Oczywiście wśród klas sprzężoności znajduje się dokładnie $q-1$ klas jednoelementowych, złożonych z elementów centrum wyłączywszy 0. Co więcej, centralizator C_g jest podpierścieniem R zawierającym podciało $Z(R)$. A zatem pierścień C_g jest przestrzenią liniową nad $Z(R)$; niech $n_g = \dim_{Z(R)} C_g < n = \dim_{Z(R)} R$. Mamy więc

$$q^n - 1 = q - 1 + \sum_{|C(g)|\neq 1} \frac{q^n - 1}{q^{n_g} - 1}$$

Liczba $\frac{q^n-1}{q^{n_g}-1}$ jest naturalna tylko wtedy, gdy $n_g|n$. Ponadto wtedy $\frac{X^n-1}{X^{n_g}-1}$ jest wielomianem o współczynnikach całkowitych. Ale wielomiany $X^{n_g}-1, \Phi_n(X)$ są względnie pierwsze, wobec czego wielomian X^n-1 jest podzielny przez ich iloczyn $(X^{n_g}-1)\Phi_n(X)$. Stąd natychmiast $\Phi_n(q)|\frac{q^n-1}{q^{n_g}-1}$. Z równości powyżej wynika więc, że $\Phi_n(q)$ dzieli $q-1$. Jednak, zakładając że centrum jest właściwym podciałem pierścienia R, i.e. $n > 1$, otrzymujemy sprzeczność, bowiem dla dowolnego pierwiastka z jedynki $\xi \neq 1$ mamy $|q-\xi| > |q-1|$ (zobaczyć to geometrycznie!), toteż $\Phi_n(q) > |q-1|$. Stąd $n = 1$, co kończy dowód. ■

4 Ogólne rozszerzenia cyklotomiczne

Odchodzimy od szczególnego przypadku ciała liczb wymiernych. Niech $\mathbb{K}$ będzie ciałem. Zachodzi oczywiście

Twierdzenie 4.1. *Niech $\mathbb{K}$ będzie ciałem, zaś U_n oznacza grupę pierwiastków z jedynki stopnia n w ciele $\mathbb{K}$. Wtedy grupa U_n jest cykliczna.*

Dowód. Oczywiście grupa U_n jest skończoną podgrupą $\mathbb{K}^*$. Niech N oznacza wykładnik tej grupy (tj. maksymalny rząd elementów w U_n). Wtedy elementy tej grupy są pierwiatkami wielomianu $X^N - 1$ w $\mathbb{K}[X]$. Zatem $|U_n| \leq N$; z drugiej strony w U_n mamy element rzędu N, skąd wniosek, że $|U_n| = N$, ■

Uwaga 4.1. *Jest faktem ogólnym, że podgrupa skończona grupy multiplikatywnej ciała $\mathbb{K}$ jest cykliczna, co wynika z tego samego argumentu, co powyżej.*

Uwaga 4.2. *Przypuśćmy, że ζ jest pierwiastkiem pierwotnym stopnia n (w ciele $\mathbb{K}$). Wówczas $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ są parami różnymi (bo ζ jest pierwotny) pierwiastkami stopnia n z jedynki w $\mathbb{K}$. Zatem wielomian $X^n - 1 \in \mathbb{K}[X]$ jest wówczas rozdzielczy. W drugą stronę, jeśli ten wielomian jest rozdzielczy, to grupa U_n jest cykliczna rzędu n.*

W naszych dalszych rozważaniach zakładamy, że wielomian $X^n - 1$ jest rozdzielczy w $\mathbb{K}[X]$ (równoważnie charakterystyka $\mathbb{K}$ jest zerowa lub równa p, przy czym $(p, n) = 1$)

Zauważmy, że jeśli ζ jest pierwiastkiem pierwontym stopnia n z jedynki, to rozszerzenie $\mathbb{K} \subset \mathbb{K}(\zeta)$ jest rozszerzeniem Galois, gdyż jest ciałem rozkładu wielomianu $X^n - 1$.

Lemat 4.1. *Niech $\varphi \in Gal\big(\mathbb{K}(\zeta) : \mathbb{K}\big)$. Istnieje wówczas $k \in \mathbb{N}$ takie, że $(k, n) = 1$ i $\varphi(\zeta) = \zeta^k$.*

Dowód. Wiemy, że $\varphi(\zeta)$ jest pierwiastkiem stopnia n z jedynki. Co więcej, jest on pierwotny, bo gdyby $\varphi(\zeta)^m = 1$ dla $m < n$, to mielibyśmy $\zeta^m = 1$ dla $m < n$, co nie ma miejsca. Zatem $\varphi(\zeta) = \zeta^k$ dla pewnego $k \in \mathbb{N}$ względnie pierwszego z n. ■

Wniosek 4.1. *Rozważmy rozszerzenie cyklotomiczne $\mathbb{K} \subset \mathbb{K}(\zeta)$. Grupa Galois tego rozszerzenia $Gal\big(\mathbb{K}(\zeta) : \mathbb{K}\big)$ zanurza się w $\mathbb{Z}_n^*$.*

Dowód. Niech $\varphi \in Gal\big(\mathbb{K}(\zeta) : \mathbb{K}\big)$. Każdemu takiemu automorfizmowi przypisujemy $k \mod n$, gdzie $k \in \mathbb{N}$ jest takie, że $\varphi(\zeta) = \zeta^k$ (poprzedni lemat mówi, że $k \mod n \in \mathbb{Z}_n^*$). Oczywiście $\zeta^i = \zeta^j$ wtedy i tylko wtedy, gdy $i \equiv j \mod n$, więc takie odwzorowanie jest dobrze określone. Ponadto jest to oczywiście injektywny homomorfizm grupy $Gal\big(\mathbb{K}(\zeta) : \mathbb{K}\big)$ w grupę $\mathbb{Z}_n^*$. ■

Wniosek 4.2. *Każde rozszerzenie cyklotomiczne $\mathbb{K} \subset \mathbb{K}(\zeta)$ jest abelowe.*

Wiemy, że jeśli $\mathbb{K} = \mathbb{Q}$ zanurzenie określone powyżej jest w istocie izomorfizmem grup. Oczywiście, nie w każdym przypadku jest to prawdą; jeśli $\mathbb{K} = \mathbb{R}$, to grupa Galois nietrywialnego rozszerzenia cyklotomicznego jest izomorficzna z $\mathbb{Z}_2$.

Twierdzenie 4.2. *Niech p będzie liczbą pierwszą, względnie pierwszą z n. Wówczas obrazem znurzenia $Gal\big(\mathbb{Z}_p(\zeta) : \mathbb{Z}_p\big) \to \mathbb{Z}_n^*$ jest $\langle p \mod n \rangle$.*

Dowód. Wiadomo z teorii ciał skończonych, że automorfizm φ_p ciała $\mathbb{Z}_p(\zeta)$ zadany wzorem $\varphi_p(x) = x^p$ dla $x \in \mathbb{Z}_p(\zeta)$ jest generatorem grupy automorfizmów tego ciała $Gal\big(\mathbb{Z}_p(\zeta) : \mathbb{Z}_p\big)$. Zatem, obrazem naszego zanurzenia będzie podgrupa $\mathbb{Z}_n^*$ generowana przez obraz automorfizmu φ_p; ten zaś jest równy $p \mod n$, co kończy dowód. ■

Powyższe twierdzenie odsłania przed nami stopień rozszerzenia $\mathbb{Z}_p \subset \mathbb{Z}_p(\zeta)$!

Wniosek 4.3. *Nieh $\mathbb{Z}_p \subset \mathbb{Z}_p(\zeta)$ będzie rozszerzeniem o pierwiastek pierwotny stopnia n, gdzie $(n, p) = 1$. Wówczas $|\mathbb{Z}_p(\zeta) : \mathbb{Z}_p| = o(p)$, gdzie $o(p)$ oznacza rząd elementu $p \mod n$ w grupie $\mathbb{Z}_n^*$.*

Z tych rozważań wynika, że **zwykle** zanurzenie $Gal\big(\mathbb{Z}_p(\zeta):\mathbb{Z}_p\big) \to \mathbb{Z}_n^*$ nie będzie surejktywne. Istotnie, warunkiem koniecznym i dostatecznym jest to, aby $p \mod n$ było generatorem grupy $\mathbb{Z}_n^*$, a przecież nie dla każdego n grupa $\mathbb{Z}_n^*$ jest cykliczna! (np. $n = 8$, $n = 12$)

Twierdzenie 4.2 uogólnia się łatwo na ciała skończone.

Twierdzenie 4.3. *Niech $\mathbb{F}_q$ będzie q-elementowym ciałem skończonym. Niech ζ będzie pierwiastkiem pierwotnym stopnia n, gdzie $(n,q) = 1$. Wtedy obrazem zanurzenia $Gal\big(\mathbb{F}_q(\zeta):\mathbb{F}_q\big) \to \mathbb{Z}_n^*$ jest $\langle q \mod n\rangle$.*

Dowód. Przekształcenie: $x \to x^q$ jest automorfizmem ciała $\mathbb{F}_q(\zeta)$ będący identycznością na $\mathbb{F}_q$. Co więcej, generuje on grupę $Gal\big(\mathbb{F}_q(\zeta):\mathbb{F}_q\big)$ (przypominam; jeżeli stopień rozszerzenia $\mathbb{F}_q \subset \mathbb{F}_q(\zeta)$ jest równy m, to ciało $\mathbb{F}_q(\zeta)$ jest ciałem rozkładu wielomianu $X^{p^{mn}} - X \in \mathbb{Z}_p[X]$, gdzie $q = p^n$). Stąd teza. ■

Wróćmy teraz do wielomianów cyklotomicznych. Wiemy już, że $\Phi_n \in \mathbb{Z}[X]$ jest wielomianem nierozkladalnym nad $\mathbb{Q}$. W dowodzie patrzyliśmy na ten wielomianem redukując jego współczynniki $\mod p$, gdzie p była liczbą pierwszą względnie pierwszą z n. W pewnym momencie zastanawialiśmy się, czy taki zredukowany wielomian $\pi^*(\Phi_n) \in \mathbb{Z}_p[X]$ jest nierozkładalny nad $\mathbb{Z}_p$. Okazuje się, że jesteśmy w stanie dokładnie powiedzieć, kiedy tak będzie.

Twierdzenie 4.4. *Niech p będzie liczbą pierwszą niedzielącą n. Nierozkładalne czynniki wielomianu $\pi^*(\Phi_n) \in \mathbb{Z}_p[X]$ są parami różne, a stopień każdego z nich jest równy rzędowi elementu $p \mod n$ w grupie $\mathbb{Z}_n^*$.*

Dowód. Z warunku $(p,n) = 1$ wynika, że wielomian $\pi^*(X^n - 1)$ jest rozdzielczy nad $\mathbb{Z}_p$. Co więcej, jeśli α jest pierwiastkiem $\pi^*(\Phi_n)$ w pewnym rozszerzeniu ciała $\mathbb{Z}_p$, to α jest pierwiastkiem pierwotnym stopnia n (znowu to wynika z rodzielczości $\pi^*(X^n-1)$). Jeśli teraz, wielomian $f \in \mathbb{Z}_p[X]$ jest nierozkładalnym czynnikiem wielomianu $\pi^*(\Phi_n)$, zaś α jakimś jego pierwiastkiem, to $\deg f = |\mathbb{Z}_p(\alpha):\mathbb{Z}_p| = o(p)$ z wniosku 4.3. ■

Powyższe twierdzenie zaopatrza nas w warunek konieczny i dostateczny na to, by wielomian $\Phi_n \in \mathbb{Z}[X]$ był także nierozkładalny po redukcji współczynników $\mod p$.

Wniosek 4.4. *Wielomian $\pi^*(\Phi_n) \in \mathbb{Z}_p[X]$ jest nierozkładalny wtedy i tylko wtedy, gdy liczba pierwsza p nie dzieli n oraz $p \mod n$ jest generatorem grupy $\mathbb{Z}_n^*$. W szczególności, warunkiem koniecznym jest to, aby grupa $\mathbb{Z}_n^*$ była grupą cykliczną.*

Dowód. Najpierw zobaczmy następujący fakt. Jeśli $(p,m) = 1$, to $\Phi_{p^r m}(X) = \frac{\Phi_m(X^{p^r})}{\Phi_m(X^{p^{r-1}})}$ w $\mathbb{Z}[X]$. Rzeczywiście, niech α będzie pierwiastkiem wielomianu

$\Phi_m(X^{p^r}) \in \mathbb{Z}[X]$. Wtedy α^{p^r} jest pierwiastkiem pierwotnym stopnia m z jedynki. Przypuśćmy, że $\alpha^{p^{r-1}}$ **nie jest** pierwiastkiem pierwotnym stopnia m z jedynki. Gdyby $\alpha^k = 1$ dla pewnego $k = p^s l < p^r m$, to:

1. nie może być $l < m$, bo α^{p^r} jest pierwotny stopnia m
2. nie może być $l = m$, bo $\alpha^{p^{r-1}}$ nie jest pierwiastkiem pierwotnym stopnia m

Stąd też $k \geq p^r m$, czyli α jest pierwotny stopnia $p^r m$. Jeśli zaś β jest takie, że $\beta^{p^{r-1}}$ jest pierwiastkiem pierwontym stopnia m, to β^{p^r} jest pierwotny stopnia m. Istotnie, jeśli $\beta^{p^r k} = 1$, to $m|pk$, skąd $m|k$ z $(p, m) = 1$.

Jeśli więc wielomian $\pi^*(\Phi_n)$ jest nierozkładalny, to musi być $(n, p) = 1$; gdyby tak nie było, to na mocy udowodnionego faktu mielibyśmy $\pi^*\big(\Phi_{p^r m}(X)\big) = \pi^*\big(\Phi_m(X)\big)^{p^r - p^{r-1}}$. Co więcej, na mocy twierdzenia 4.4 , rząd elementu $\langle p \bmod n\rangle$ musi być równy $\varphi(n)$. Na odwrót, jeśli $(p, n) = 1$ i rząd elementu $p \bmod n$ w $\mathbb{Z}_n^*$ jest równy $\varphi(n)$, to znowu z twierdzenia 4.4 czynniki nierozkładalne $\pi^*(\Phi_n)$ mają stopień $\varphi(n) = \deg \Phi_n$, co kończy dowód. ■

Proszę zauważyć, że z powyższego wniosku wynika, że istnieją wielomiany cyklotomiczne Φ_n o tej własności, że po redukcji modulo p dla każdej liczby pierwszej p, otrzymamy **zawsze** wielomian rozkładalny w $\mathbb{Z}_p[X]$! Najmniejszym (co do stopnia) wielomianem o tej własności jest wielomian $\Phi_8(X) = X^4 + 1$.