Zadanie 9d

Zauważmy, że każdą niezerową liczbę $a \in \hat{\mathbb{Z}_p}$ można zapisać jako $a = up^k$ gdzie u jest odwracalne. Istotnie, skoro liczba a jest niezerowa, to jest niezerowa modulo pewne p^k. Weźmy najmniejsze takie l i ustalamy k na $l-1$. Wtedy oczywiście dla każdego l mamy $p^k | a \mod p^l$, zatem bardzo łatwo możemy zdefiniować $u = a/p^k$, gdyż mamy $\mathbb{Z}_{p^{l-k}} \cong \mathbb{Z}_{p^l}/\langle p^k \rangle \twoheadrightarrow \mathbb{Z}_{p^{l-1}}/\langle p^k \rangle \cong \mathbb{Z}_{p^{l-k-1}}$ dla $l > k$, gdyż $\langle p^k \rangle \subseteq \ker(\mathbb{Z}_{p^l} \to \mathbb{Z}_{p^{l-1}})$, zatem mamy nić, więc u jest dobrze określone (intuicyjnie: skreślamy k ostatnich zer z zapisu liczby a i widzimy, że jest nadal dobrze). Teraz jednak u jest odwracalne na mocy zadania 5.

Stąd widzimy, że dla dowolnego ideału I możemy wziąć zbiór generujący G (np. cały ideał), po czym w każdym elemencie wziąć tylko jego p^k (bo można odwracać u). Łatwo stąd widać, że każdy niezerowy ideał w $\hat{\mathbb{Z}_p}$ jest postaci (p^k) dla pewnego k (najmniejsze z k występujących w zbiorze generatorów).

Oczywiście jedyny niezerowy ideał pierwszy to (p), gdyż w każdym innym mamy $p^{k-1}, p \notin (p^k)$, lecz $p^{k-1}p = p^k \in (p^k)$, jest to też więc jedyny ideał maksymalny.

Ponadto pierwszy jest ideał (0), gdyż w liczbach p-adycznych nie ma dzielników zera, gdyż dla dowolnych a, b mamy $a = u_a p^{k_a}$, $b = u_b p^{k_b}$, skąd $ab = u_a u_b p^{k_a + k_b}$ no i łatwo widać, że modulo $p^{k_a+k_b+1}$ ta liczba jest niezerowa.

Pierścień ilorazowy $\hat{\mathbb{Z}_p}/(0)$ jest oczywiście izomorficzny z $\hat{\mathbb{Z}_p}$. Zajmijmy się więc pierścieniem $\hat{\mathbb{Z}_p}/(p)$.

Zauważmy, że przekształcenie f biorące liczbę p-adyczną modulo p jest homomorfizmem. Ponadto zeruje się ono jedynie dla liczb z (p), zatem $\hat{\mathbb{Z}_p}/(p) \cong \operatorname{im} f$, lecz $\operatorname{im} f \cong \mathbb{Z}_p$ praktycznie wprost z definicji liczb p-adycznych. Zatem ten pierscień ilorazowy to $\mathbb{Z}_p$.

Zadanie 14

Zauważmy, że oczywiście $I := (x^2 + y^2 + 10y, x^2 - y) \subseteq (x^2, y)$ (gdyż każdy z generatorów tam należy). Ponadto $x \notin (x^2, y)$, zatem $xy + 11x \notin (x^2, y)$, zatem $xy + 11x \notin I$. Jednakże $(xy+11x)^2 = x^2y^2 + 22x^2y + 121x^2 = (y^2 + 21y + 110)(x^2 - y) + (y + 11)(x^2 + y^2 + 10y) \in I$.

Ale zauważmy, że jeśli $P \supseteq I$ będzie ideałem pierwszym, to ponieważ $(xy + 11x)^2 \in P$, to $xy + 11x \in P$, zatem I nie może być przecięciem ideałów pierwszych, a co dopiero maksymalnych.

Zadanie 15

Łatwo widać, że działanie to zachowuje potęgi x oraz y, zatem jednomiany przesyła na te same jednomiany, ale z inną stałą. Dokładniej, mamy, że $x^a y^b \mapsto \xi^{a-b} x^a y^b$. Zatem w zbiorze F punktów stałych działania niezerowe współczynniki mogą być jedynie przy takich jednomianach, w których $n | a - b$. Co więcej, dowolny wielomian złożony z takich jednomianów jest punktem stałym danego działania. Oczywiście jednak suma takich wielomianów jest nadal tej postaci, element przeciwny także, wielomiany 0 i 1 także, a ponadto $x^a y^b \cdot x^c y^d = x^{a+c} y^{b+d}$, zatem jeśli zachodziło $n | a - b$ i $n | b - d$, to oczywiście mamy $n | (a + c) - (b + d)$, czyli iloczyn nie wyprowada poza jednomiany z F, zatem iloczyn wielomianów z F także jest w F, z rozdzielności. Zatem F jest podpierścieniem.

Określmy przekształcenie:

$$\begin{aligned} \mathbb{C}[p, q, r] &\xrightarrow{\phi} \mathbb{C}[x, y] \\ p^k q^l r^m &\mapsto x^{kn+m} y^{ln+m} \end{aligned}$$

Ponieważ $n | (kn + m) - (ln + m)$, to $\operatorname{im} \phi \subseteq F$. Ponadto zauważmy, że wszystkie generatory F (tj. jednomiany $x^a y^b$ dla $n | a - b$) są osiągane. Istotnie, jeśli $a > b$, to bierzemy $m = b$, $k = \frac{a-b}{n}$, $l = 0$, jeśli zaś $a < b$ to $m = a$, $k = 0$, $l = \frac{b-a}{n}$. Zatem $\operatorname{im} \phi \cong F$.

Teraz popatrzmy na $\ker \phi$. Twierdzę, że $\ker \phi = (r^n - pq)$. Oczywiście $\phi(r^n - pq) = 0$. Niech teraz $P \in \ker \phi$. Wtedy oczywiście możemy P rozbić na sumę jednomianów i pogrupować je w bloki takich jednomianów, które (pomijając stałą) dają to samo po przejściu przez ϕ. Jeżeli $\phi(p^k q^l r^m) = \phi(p^{\hat{k}} q^{\hat{l}} r^{\hat{m}})$ to mamy oczywiście $kn + m = \hat{k}n + \hat{m}$ oraz $ln + m = \hat{l}n + \hat{m}$, skąd odejmując stronami i dzieląc przez n uzyskujemy $k - l = \hat{k} - \hat{l}$, skąd oznaczając $k - \hat{k} = l - \hat{l} = c$ mamy, że $\hat{m} - m = nc$. Gdy teraz mamy kombinację liniową takich jednomianów, to możemy łatwo wziąć ten o największym wykładniku przy r, od naszej sumy odjąć odpowiednio przemnożony wielomian $r^n - pq$ i uzyskać kombinację z mniejszym maksymalnym wykładnikiem przy r. Zauważmy, że na końcu nie mógł nam zostać pojedynczy jednomian ani niezerowa stała, gdyż zaczęliśmy z kombinacją z jądra i odejmowaliśmy elementy z jądra, zatem to na końcu też jest z jądra, a żaden pojedynczy wielomian ani niezerowa stała nie są w $\ker \phi$ (bo $kn + m = ln + m = 0$ wtedy i tylko wtedy, gdy $k = l = m = 0$, a wyrazy wolne są zachowywane przez ϕ). Zatem uzyskaliśmy, że suma jednomianów należy do $(r^n - pq)$, czyli $P \in (r^n - pq)$.

Zatem z tw. o izomorfizmie mamy $\mathbb{C}[p, q, r]/(r^n - pq) \cong F$.

Zadanie 16

Niech $p \in I, q \in J$ będą takie, że $p + q = 1$.

Część a

Oczywiście $IJ \subseteq I$, $IJ \subseteq J$, zatem $IJ \subseteq I \cap J$.

Zauważmy, że teza jest nieprawdą jeśli przyjmiemy definicję IJ jak w treści. Istotnie, niech $R = \mathbb{Z}[x, y]$, $I = (x, y)$, $J = (x-1, y)$. Wtedy $x^2-x \in IJ$, $y^2 \in IJ$, lecz $x^2-x+y^2 \notin IJ$, gdyż jeśli byłby on w IJ, to mielibyśmy rozkład tego wielomianu na iloczyn dwóch niestałych wielomianów. Patrząc na niego jako na wielomian jednej zmiennej x z parametrem y łatwo widzimy, że taki rozkład musi mieć oba czynniki liniowe ze względu na x (gdyż żaden ze składników nie może być stały względem x, gdyż to by znaczyło, że y dzieli ten wielomian). Analogicznie pokazujemy, że oba składniki są liniowe względem y. Oczywiście jeden z nich musi mieć zerowy wyraz wolny. Zapisując jednak $x^2 - x + y^2 = (ax + by + c)(dx + ey) = bey^2 + (ae + bd)xy + cey + adx^2 + cdx$, skąd $be = 1, ce = 0, cd = -1$, lecz $ce = 0 \implies c = 0 \vee e = 0 \implies be = 0 \vee cd = 0$, co jest sprzecznością.

Zatem IJ nie byłoby ideałem, a co dopiero równe $I \cap J$. Zatem przyjmijmy definicję $IJ := (\{xy : x \in I \wedge y \in J\})$. Teraz jeśli $a \in I \cap J$, to $a = a \cdot (p + q) = ap + aq \in JI + IJ = IJ$.

Część b

Niech $x = aq+bp$. Wtedy mamy, że $x-a = aq+bp-a = a(1-p)+bp-a = a-ap+bp-a = -ap+bp \in I$, analogicznie $x - b \in J$.