Zadanie 24

Zauważmy, że $\mathfrak{m}_i \not\subseteq \mathfrak{m}_{i+1}$, gdyż inaczej nie byłyby to parami różne ideały maksymalne. Zatem istnieje $a_i \in \mathfrak{m}_i$ takie, że $a_i \notin \mathfrak{m}_{i+1}$. Analogicznie istnieje $a_n \in \mathfrak{m}_n$ takie, że $a_n \notin \mathfrak{m}_1$.

Rozpatrzmy $a = a_1 \dots a_n$. Oczywiście $a = (a_1 \dots a_{i-1} a_{i+1} \dots a_n) a_i \in \mathfrak{m}_i$. Zatem $a \in I$, skąd gdyby I był pierwszy, mielibyśmy $\exists_i a_i \in I$, czyli w szczególności $a_i \in \mathfrak{m}_{(i \bmod n)+1}$, wbrew założeniu.

Zadanie 28

Zauważmy, że $p = 2, 3$ nie spełniają żadnego z warunków w zadaniu (ich reszty mod 6 to ani nie 1 ani nie 5), zatem załóżmy dalej, że $p \notin \{2, 3\}$. Zauważmy, że oczywiście $R = \mathbb{Z}[\sqrt{-3}]/(p) \cong (\mathbb{Z}[x]/(x^2+3))/(p) \cong \mathbb{Z}/(p)[x]/(x^2+3)$. Zauważmy dalej, że równanie $\left(\frac{x-1}{2}\right)^3 = 1 \iff (x-1)^3 = 8 \iff x^3 - 3x^2 + 3x - 9 = 0 \iff (x-3)(x^2+3) = 0$. Zatem w $\mathbb{Z}/(p)$ istnieje pierwiastek kwadratowy z -3 wtedy i tylko wtedy gdy istnieje nietrywialny pierwiastek trzeciego stopnia z jedności (ewentualny wiszący tu przypadek $x = 3$ nie daje pierwiastka kwadratowego z -3, gdyż $3^2 + 3 = 12$, co jest niezerowe modulo p różne od 2 i 3). Jednak na mocy tw. Lagrange'a i tw. Cauchy'ego taki pierwiastek istnieje wtedy i tylko wtedy gdy $3 \mid p - 1$.

Zatem gdy $p \equiv 5 \pmod 6$ to nie ma pierwiastka wielomianu x^2+3, zatem jest on nierozkładalny (bo stopnia 2), zatem $R \cong \mathbb{Z}/(p)[x]/(x^2+3) \cong GF(p^2)$. Gdy zaś x^2+3 ma pierwiastek to ma dwa (i to różne, gdyż pochodna, czyli $2x$ zeruje się tylko w zerze, a zero nie jest pierwiastkiem tego wielomianu (bo $p \neq 3$)), zatem z twierdzenia Sun Tzu mamy: $\mathbb{Z}/(p)[x]/(x^2+3) \cong \mathbb{Z}/(p)[x]/(x-\alpha) \times \mathbb{Z}/(p)[x]/(x-\beta) \cong GF(p)^2$.

Zadanie 29

Mamy $f^* = (\circ f)$, tj. $f^*(v) = v \circ f$.

Część a

Zauważmy, jak wygląda $f^* : \mathfrak{m}_b/\mathfrak{m}_b^2 \to \mathfrak{m}_a/\mathfrak{m}_a^2$. Zauważmy, że w dziedzinie mamy tak naprawdę wielomiany liniowe, gdyż zabijamy część kwadratową i wyższe, a część stała jest zerowa (w b). Analogicznie w przeciwdzienie (tam mamy zerowość w a). Zatem przechodząc do f^* na ilorazach widzimy, że tak naprawdę interesuje nas to, co f robi z częścią liniową, czyli dokładnie to, jaka jest jego pochodna (która jest z definicji liniowym przybliżeniem). Zatem $f^*([v]) = [v \circ f] = [v \circ (Df)]$. Ponadto jeśli się ograniczymy do brania v liniowych (a możemy, bo część kwadratową i wyższe zabijamy), to $[v \circ (Df)] = 0 \iff v \circ (Df) = 0$, gdyż transformacja liniowa współrzędnych nie zrobi nam wielomianu wyższego stopnia.

No ale oczywiście jak wiemy z pierwszego semestru GAL-u, $\circ(Df) = (Df)^*$ jest monomorfizmem wtedy i tylko wtedy, gdy Df jest epimorfizmem, czyli ma rząd r.

Część b

Niech $\psi : \mathfrak{m}_a/\mathfrak{m}_a \to \overline{\mathfrak{m}}_a/\overline{\mathfrak{m}}_a^2$ będzie takie, że $\psi([f]) = [[f]]$. Oczywiście jeśli $[f] = [0]$, czyli f jest sumą kwadratów wielomianów z $\mathfrak{m}_a$, to w $\overline{\mathfrak{m}}_a$ to też będzie suma kwadratów wielomianów, zatem $[[f]] = 0$. Ponadto ψ dobrze się zachowuje przy działaniach pierścienia, zatem jest dobrze określone i homomorfizmem.

Na mocy twierdzenia o izomorfizmie wystarczy wykazać, że ciąg

$$\mathfrak{m}_b/\mathfrak{m}_b^2 \xrightarrow{\circ(Df)} \mathfrak{m}_a/\mathfrak{m}_a^2 \xrightarrow{\psi} \overline{\mathfrak{m}}_a/\overline{\mathfrak{m}}_a^2$$

jest dokadny.

Oczywiście jeśli weźmiemy $[v] \in \mathfrak{m}_b/\mathfrak{m}_b^2$ dla v – wielomian liniowy, to $[v \circ Df] = [v \circ f]$, zatem $\psi([v \circ Df]) = [[v \circ f]]$, lecz $v \circ f$ jest kombinacją liniową wielomianów f_i o zerowym wyrazie wolnym przy ustawieniu środka układu współrzędnych w b (bo $v(b) = 0$), zatem jest to kombinacja wielomianów $f_i - b_i$, zatem $[v \circ f] = 0$ w $k[x_1, \dots, x_n]/(f_1 - b_1, \dots, f_r - b_r)$.

Pozostaje sprawdzić, że jeśli $\psi([u]) = 0$ dla pewnego u – liniowego zerującego się w a, to $u = v \circ Df$ dla pewnego v liniowego zerującego się w b. Warunek $\psi([u]) = 0$ mówi, że $[[u]] = 0$, czyli $[u]_{(f_1-b_1,\dots,f_r-a_r)} \in \overline{\mathfrak{m}}_a^2$, zatem mamy, że u jest sumą: kwadratów pewnych wielomianów ($\overline{\mathfrak{m}}_a^2$) oraz odpowiednich wielomianowych wielokrotności wielomianów $f_1 - b_1, \ldots, f_r - b_r$ (zauważmy, że $f_i - b_i$ jest wielomianem o zerowym wyrazie wolnym). Jednak w u interesuje nas jedynie część conajwyżej liniowa, zatem mamy, że u jest kombinacją liniową części liniowych wielomianów $f_i - b_i$, zatem jest to pewna kombinacja wierszy macierzy Df, czyli $u = \nu \circ (Df)$ dla pewnego ν (swobodnie tu zamieniam funkcję, wielomian i macierz, gdyż raczej nie prowadzi to do nieporozumień), gdzie u jest we współrzędnych o środku w a, zaś ν jest we współrzędnych o środku w b, gdyż mnożenie przez Df przeprowadza nas w inny układ współrzędnych. Oczywiście stąd $\nu(b) = 0$. Zatem $\operatorname{im}(\circ(Df)) = \ker\psi$, czyli ciąg ten jest dokładny.

Zadanie 30

Zauważmy, ze $\nu(a + b\alpha) = |a^2 + ab(\alpha + \beta) + b^2\alpha\beta| = |a^2 + ab - b^2|$, gdzie ostatnia róœność wynika ze wzorów Viety. Multiplikatywność ν jest oczywista. Gdy określimy $\overline{a + b\alpha} = a + b\beta$, to widzimy, że $\bar{\cdot}$ jest homomorfizmem, gdyż $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(x^2 - x - 1) \cong \mathbb{Z}[\beta]$ (z nierozkładalności $x^2 - x - 1$ – wprawdzie $\mathbb{Z}$ nie jest ciałem, ale jednak $x^2 - x - 1$ ma współczynnik wiodący jeden, a zatem ten sam dowód, który daje wyżej wymienione izomorfizmy nad $\mathbb{Q}$ działa też nad $\mathbb{Z}$) i złożenie tych izomorfizmów daje $\bar{\cdot}$. Mamy jednak $\nu(x) = |x\overline{x}|$, co jest multiplikatywne z multiplikatywności $\bar{\cdot}$ oraz modułu rzeczywistego.

Pozostaje wykazać warunek z dzieleniem z resztą. Załóżmy więc, że mamy dane $a + b\alpha$ i $c + d\alpha$, przy czym to drugie jest niezerowe. Dzieląc tak jak liczby rzeczywiste i usuwając niewymierność z mianownika uzyskujemy $\frac{a+b\alpha}{c+d\alpha} = p + q\alpha$, gdzie $p, q \in \mathbb{Q}$. (najpierw sprowadzamy do postaci $\hat{p} + \hat{q}\sqrt{5}$, a potem stosownym przekształceniem liniowym piszemy $\hat{p} + \hat{q}\sqrt{5} = p + q\alpha$).

Niech teraz x, y będą liczbami całkowitymi najbliższymi p, q. Zauważmy teraz, że tak jak na wykładzie, wystarczy pokazać, że $\nu((p - x) + (q - y)\alpha) < 1$, gdzie waluację rozszerzamy na $\mathbb{Q}[\alpha]$ w oczywisty sposób.

Ale to jest prawda, gdyż $|p-x|, |q-y| \leqslant \frac{1}{2}$, zatem $\nu((p-x)+(q-y)\alpha) \leqslant |(p-x)^2|+|(p-x)(q-y)|+|(q-y)^2| \leqslant \frac{3}{4} < 1$.