Algebra II (ISIM), lista 8 (poniedziałek 11.12.2017, 12:15-14:00, sala 5 w II).

Teoria: Pierścienie przemienne z 1: definicja, przykłady. Pierścienie formalnych szeregów potęgowych, wielomianów, funkcji ciągłych, macierzy, boolowskie, modulo, $End(G)$. Produkt pierścieni. Grupa R^* elementów odwracalnych (jednostek) pierścienia. Podzielność i stowarzyszenie. Dzielnik zera. Homomorfizmy pierścieni. Ideał. Pierścień ilorazowy. Zasadnicze twierdzenie o homomorfizmie pierścieni, twierdzenie o faktoryzacji homomorfizmu. Ideał główny, ideał skończenie generowany. Pierścienie ideałów głównych: $\mathbb{Z}, K[X], \mathbb{Z}_n$. Funkcja i twierdzenie Eulera.

R, R' oznaczaja pierścienie przemienne z jednością.

1. $-$ Udowodnić Uwagę 9.2 z wykładu, odwołując się bezpośrednio do aksjomatów pierścienia.

2. $-$ Udowodnić, że R^* jest grupą.

3. (a) Niech $+, \cdot$ będą działaniami w zbiorze A takimi, że $(A, +)$ jest grupą, zaś działanie $\cdot$ jest łączne, obustronnie rozdzielne względem $+$ i ma element neutralny $1 \in A$. Wykazać, że wtedy $(A, +, \cdot)$ jest pierścieniem. (wsk: wystarczy udowodnić przemienność $+$).
   (b) Załóżmy, że $(A, +, \cdot)$ jest pierścieniem, w którym grupa addytywna $(A, +)$ jest cykliczna. Udowodnić, że ten pierścień jest przemienny. Czy jest to pierścień z jednością?

4. $-$ Niech $a, b \in \mathbb{R}$ oraz $I \lhd R$. Udowodnić, że:
   (a) $a|b \iff (b) \subseteq (a)$
   (b) Jeśli $a \sim b$, to $a \in I \iff b \in I$.
   (c) $a \sim b \iff (a) = (b)$.
   (d) $a \sim b \iff a = \varepsilon b$ dla pewnego $\varepsilon \in R^*$. (e) I jest właściwy $\iff 1 \notin I$.

5. * (a) Załóżmy, że R jest pierścieniem niekoniecznie przemiennym, w którym zachodzi równość $x^2 = x$. Udowodnić, że wtedy w R zachodzi równość $x+x = 0$ oraz R jest przemienny.
   (b) Załóżmy, że R jest pierścieniem boolowskim. Udowodnić, że istnieje algebra Boole'a A taka, że $R \cong (A, \triangle, \wedge)$. (wsk: zacząć od algbery Boole'a $A = (A, \wedge, \vee, ', 0, 1)$. Zauważyć, że operacje $\vee$ i $'$ można zdefiniować w pierścieniu boolowskim $(A, \triangle, \wedge)$).
   (c) Sprawdzić, że pojęcie ideału w algebrze Boole'a A pokrywa się z pojęciem ideału (w sensie teorii pierścieni) w tejże algebrze traktowanej jako pierścień boolowski.

6. Załóżmy, że $a \in \mathbb{Z}_n \setminus \{0\}$. Udowodnić, że
   (a) a jest odwracalny $\iff NWD(a, n) = 1$.
   (b) a jest dzielnikiem zera $\iff NWD(a, n) > 1$.

7. (a) Udowodnić, że $\mathbb{R}[\![X]\!]^*$ składa się z szeregów z niezerowym wyrazem wolnym.
   (b) Obliczyć szeregi odwrotne do szeregów $\sum_i 2^i X^i$ i $\sum_i X^i$ w pierścieniu $\mathbb{R}[\![X]\!]$.

8. Załóżmy, że R jest pierścieniem ideałów głównych oraz $f : R \to R'$ jest epimorfizmem pierścieni. Udowodnić, że R' też jest pierścieniem ideałów głównych. W szczególności każdy pierścień $\mathbb{Z}_n$ jest pierścieniem ideałów głównych.

9. $-$ Wypisać klasy stowarzyszenia w pierścieniu $\mathbb{Z}_{12}$. Wypisać wszystkie ideały w tym pierścieniu oraz sporządzić diagram Hassego dla relacji inkluzji między nimi.

10. (a) Załóżmy, że $n, m > 0$ są względnie pierwsze, zaś $f : \mathbb{Z}_{n \cdot m} \to \mathbb{Z}_n \times \mathbb{Z}_m$ dana jest wzorem $f(k) = \langle r_n(k), r_m(k) \rangle$. Udowodnić, że f jest izomorfizmem pierścieni, korzystając z (b) i z tw. o faktoryzacji homomorfizmu.
(b)$-$ Sprawdzić, że $r_n : \mathbb{Z} \to \mathbb{Z}_n$ jest epimorfizmem pierścieni oraz $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

11. (Funkcja i twierdzenie Eulera). Dla $n > 1$ niech $\varphi(n)$ będzie liczbą liczb $0 < k < n$ względnie pierwszych z n. Udowodnić następujace stwierdzenia:
(a)$-$ $\varphi(n) = |\mathbb{Z}_n^*|$
(b) $(R \times R')^* = R^* \times R'^*$
(c) $\varphi(p^k) = (p-1)p^{k-1}$, gdzie p jest liczbą pierwszą.
(d) $\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$, gdzie $p_1, \ldots, p_k$ to różne liczby pierwsze, zaś $\alpha_i > 0$.
(e) (tw. Eulera) Gdy $n, k \in \mathbb{Z}$ sa względnie pierwsze i $k > 1$, to $n^{\varphi(k)} \equiv 1 \pmod{k}$.