- *Pierścień wielomianów*

  F-ciało. $F[x]$- *pierścień wielomianów nad ciałem* F z naturalnymi definicjami dodawania i mnożenia.

  Niech $f(x) \in F[x]$ to $f(x) = \sum_{i=0}^{n} a_i x^i$, gdzie $a_i \in F$ dla $i = 0, 1, ..., n$. *Stopień* $f(x)$ ($deg\ f(x)$) to n (jeśli $a_n \neq 0$).

  Fakt: $F[x]$ ze stopniem jako normą jest dziedziną euklidesową.

  Wielomian $f(x) \in F[x]$ jest *rozkładany* nad F jeśli istnieją niestałe wielomiany $a(x), b(x) \in F[x]$ takie, że $f(x) = a(x)b(x)$. W p.p. $f(x)$ jest nieropzkładany nad F.

  Przykład: $x^2 + 1$ jest nierozkładany nad R, ale rozkładalny nad C, bo $x^2 + 1 = (x - j)(x + j)$.

- $K \subset F$ jest *podciałem* ciała $(F, +, \cdot, 0, 1)$ jeśli

  1. $\forall\ a, b \in K \quad a - b \in K$
  2. $\forall\ a, b \in K \setminus 0 \quad a \cdot b^{-1} \in K$

  F jest *rozszerzeniem* ciała K jest K jest podciałem F.

  Przykład: Q podciało R podciało C.

- Konstrukcja rozszerzenia R do C.

  C powstaje z R przez dołaczenie j takiego, że $j^2 + 1 = 0$ Czyli w C mamy elementy postaci $a + bj$, gdzie $a, b \in R$ (bo $j^2 = -1$). Czyli $1, j$ tworzą bazę C jako przestrzeni wektorowej nad R.

  Inaczej $C = R[x]/(x^2 + 1)$.

- Ogólna konstrukcja rozszerzenia ciała F:

  $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$- wielomian nierozkładany nad F.

  Rozszerzenie F to $F[x]/(f(x)) = \left\{ \sum_{i=0}^{n-1} b_i x^i : b_0, ..., b_{n-1} \in F \right\}$.

  Przykłady: $GF(4) = GF(2^2) = Z_2[x]/(x^2 + x + 1)$,

  $GF(8) = GF(2^3) = Z_2[x]/(x^3 + x^2 + 1)$.

  Tw. $GF(p^n) = Z_p/(f(x))$, gdzie $f(x) \in Z_p[x]$ wielomian nierozkładany nad Z_p stopnia n

- Fakt: Każde ciało skończone jest rozszerzeniem pewnego ciała Z_p dla p-liczby pierszej (i tylko jednego takiego ciała)