- $(R, +, \cdot)$ z dwoma działaniami *dodawania*:

$$+ : R \times R \ni (a, b) \mapsto a + b \in R$$

i *mnożenia*

$$\cdot : R \times R \ni (a, b) \mapsto a \cdot b \in R$$

nazywamy *pierścieniem* jeśli

1. $(R, +)$ jest grupą abelową
2. działanie $\cdot$ - mnożenia jest łączne
3. zachodzą prawa rozdzielności mnożenia względem dodawania

Jeśli istnieje 1-element neutralny mnożenia to pierścień nazywamy *pierścieniem z 1 (jednością).* Jeśli działanie mnożenia jest przemienne to pierścien nazywamy *przemiennym.*

- Przykłady: $(Z, +, \cdot)$, $(2Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$, $(Z_p, +_p, \cdot_p)$, $(Z[x], +, \cdot)$, $(Q[x], +, \cdot)$, $(R[x], +, \cdot)$, $(C[x], +, \cdot)$, $(M_{n\times n}(R), +, \cdot)$, $(M_{n\times n}(C), +, \cdot)$.

- Dziedzina całkowitości to pierścień przemienny R z 1 w którym zachodzi:

$$\forall a, b, c \in R \; ab = bc \; i \; a \neq 0 \Rightarrow b = c.$$

Fakt: Pierścień przemienny z 1 jest dziedziną całkowitości wtedy i tylko wtedy , gdy nie ma dzielników zera tzn.

$$\forall a, b \in R \; ab = 0 \Rightarrow a = 0 \; lub \; b = 0.$$

Wniosek: Z_p jest dziedziną cłkowitości wtedy i tylko wtedy , gdy p jest liczbą pierwszą.

- *Ciało* to pierścień z 1 w którym elementy niezerowe tworzą grupę ze względu na mnożenie.
Przykłady: $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$, $(Z_p, +_p, \cdot_p)$, gdzie p-liczba pierwsza.
Tw. Dowolna skończona dziedzina całkowitosci jest ciałem.

- $S \subset R$ jest *podpierścieniem z 1* pierścienia z 1 R jeśli $(S, +|_{S\times S}, \cdot|_{S\times S})$ jest pierścieniem z 1.
Tw. $S \subset R$ jest *podpierścieniem z 1* pierścienia z 1 R wtedy itylko wtedy , gdy:

1. $1 \in S$
2. $\forall \; a, b \in S \;\; a - b \in S$
3. $\forall \; a, b \in S \;\; a \cdot b \in S$

Przykłady: Z podpierścień Q podpierścień R podpierścień C.

- *Homomorfizmem (morfizmem)* pierścieni z 1 R i S nazywamy funkcję $F : R \to S$ taką, że

1. $F(1) = 1$
2. $\forall \; a, b \in S \;\; F(a + b) = F(a) + F(b)$
3. $\forall \; a, b \in S \;\; F(a \cdot b) = F(a) \cdot F(b) \in S$

Izomorfizm to homomorfizm wzajemnie jednonznaczy.

- Popierścień generowany przez 1 pierścienia nietrywialnego R (tzn. $1 \neq 0$).

  Charakterystyka pierścienia R ($charR$) to rząd podgrupy grupy addytywnej pierścienia generowanej przez 1.

  Tw. Jeśli $charR = m$ to pierścień generowany przez $1 \in R$ jest izomorficzny z Z_m i jest zawarty w każdym podpierścieniu pierścienia R.

  Tw. Charakterystyka dowolnej dziedziny całkowitości jest albo liczbą pierwszą albo jest równa ∞ (0).

  Wniosek. Podpierścień generowany przez 1 dowolnego ciała skończonego jest izomorficzny z Z_p.

- $\emptyset \neq H \subset R$ jest *ideałem* w pierścieniu R jeśli

  1. $\forall\ a, b \in H \quad a + b \in H$
  2. $\forall\ a \in R \quad \forall b \in H \quad a \cdot b \in H$

  Fakt: *Jądro* homorfizmu $F : R \to S$ czyli zbiór $Ker\ F = \{a \in R : F(a) = 0\}$ jest ideałem w R.

  Fakt: Zbiór $(a) = \{xa \in R : x \in R\}$ jest ideałem (*ideał główny* elementu a).

  Uwaga. F-ciało to jedyne ideały w F to $\{0\}$ i F.

- H ideał w R. Wprowadzamy relację równowańości na R w której klasami abstakcji są zbiory $x + H = \{x + h : h \in H\}$. Wtedy zbiór wszystkich klas abstrakcji tej relacji $R/H = \{x + H : x \in R\}$ zdziałaniami następująco określonymi :

  1. $\forall\ a, b \in R \quad (a + H) + (b + H) = (a + b) + H$
  2. $\forall\ a, b \in R \quad (a + H) \cdot (b + H) = (a \cdot b) + H$

  jest pierścieniem (*pierścień ilorazowy*).

  Przykład: $Z_m = Z/(m)$.

- *Dziedziną euklidesową* nazywamy dziedzinę całkowitości D z *normą (wartościowaniem)* $v : D \to N$ taką, że

  1. $\forall\ a, b \in D \setminus 0 \quad v(a \cdot b) \geq v(a)$
  2. $\forall\ a \in D\ \forall\ b \in D \setminus 0\ \exists q \in D \quad a = b \cdot q + r\ gdzie\ r = 0\ lub\ v(r) < v(b)$

  Przykłady :

  1. $Z, v(z) = |z|$
  2. $Z[\sqrt{-1}], v(a + b\sqrt{-1}) = a^2 + b^2$
  3. wielomainy nad dziedziną całkowitości ze stopniem jako normą

  Fakt: W dziedzinie euklidesowej każdy ideał jest główny.

  Alogytm Euklidesa znajdowania największego wspólnego dzielnika a i b ($NWD(a, b)$).

  1. jeśli $a = 0$ lub $b = 0$ to $NWD(a, b) = a + b$
  2. w p.p. można założyć, że $v(b) \leq v(a)$
  3. jeśli $a = q \cdot b$ to $NWD(a, b) = b$
  4. w p.p. $a = q_1 \cdot b + r_1$, gdzie $v(r_1) < v(b)$
  5. to samo powtarzamy dla r_1 i b otrzymując $b = q_2 r_1 + r_2$
  6. to samo powtarzamy dla r_2 i r_1 otrzymując $r_1 = q_3 r_2 + r_3$ itd. aż $r_k = 0$
  7. otrzymujemy $(a) + (b) = (b) + (r_1) = (r_1) + (r_2) = ... = (r_{k-2}) + (r_{k-1}) = (r_{k-1})$
  8. stąd $NWD(a, b) = r_{k-1}$