Def Ideał $I \triangleleft P$ nazywamy maksymalnym gdy
1. $I \neq P$
2. $\forall J \triangleleft P \quad J \supset I \to J = P$.

Przykład $p\mathbb{Z} = \{k \cdot p : k \in \mathbb{Z}\}$, $p \in \mathbb{P}$
ideał maksymalny w $(\mathbb{Z}, +, \cdot)$

Tw. Jeśli P pierścień przemienny z 1, oraz $I \triangleleft P$ ideał maksym.
to P/I jest ciałem.

Przykład • $(\mathbb{Z}, +, \cdot)$ - pierścień przemienny z 1.
• $3\mathbb{Z}$ - ideał maksymalny w $\mathbb{Z}$.

Pierścień $\mathbb{Z}/3\mathbb{Z} = \{k + 3\mathbb{Z} : k \in \mathbb{Z}\} = \#$

[Uw. $k + 3\mathbb{Z} = (k \bmod 3) + 3\mathbb{Z}$ bo $k - (k \bmod 3) \in 3\mathbb{Z}$]

$\# = \{(k \bmod 3) + 3\mathbb{Z} : k \in \mathbb{Z}\}$

$\mathbb{Z}/3\mathbb{Z}$
$$\mathbb{Z}/3\mathbb{Z} = \{k + 3\mathbb{Z} : k = 0, 1, 2\} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$
dodawanie: $(k + 3\mathbb{Z}) + (l + 3\mathbb{Z}) = (k + l) + 3\mathbb{Z} = (k +_3 l) + 3\mathbb{Z}$.
mnożenie $(k + 3\mathbb{Z}) \cdot (l + 3\mathbb{Z}) = \dots = (k \cdot_3 l) + 3\mathbb{Z}$

Skrótowo notujemy:

$\mathbb{Z}_3$
$$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$$
$+ \quad k + l = k +_3 l$
$\cdot \quad k \cdot l = k \cdot_3 l$

Pierścień wielomianów nad ciałem.

- Niech K ciało. Wielomianem nad K nazywamy wyrażenie $f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$
- Największą liczbę $k \in \mathbb{N}$ taką że $a_k \neq 0$ nazywamy stopień f i oznacz $st(f)$.
- Dodawanie i mnożenie jako działanie na wyrażeniach algebr. uwzględniając że $a_i \in K$.

Tw. O dzieleniu z resztą.
Niech K - ciało.
Dla dowolnych $f, g \in K[x]$ istnieją $w, r \in K[x]$

1. $f = w \cdot g + r$
2. $st(r) < st\, g$.

Przykład $\mathbb{R}[x]$:

$f = x^3 + x + 1$

$g = x + 1$

$$
\begin{array}{l}
\quad\; x^2 - x + 2 \quad w \\
\hline
x^3 + x + 1 \; : \; x + 1 \\
-x^3 + x^2 \\
\hline
= -x^2 + x + 1 \\
- \quad -x^2 - x \\
\hline
= \quad 2x + 1 \\
\quad\;\; 2x + 2 \\
\hline
\quad\;\; -1 \quad r
\end{array}
$$

Mamy:

$$x^3 + x + 1 = (x^2 - x + 2)(x + 1) + (-1)$$

$$f = w \cdot g + r$$

Oznaczenie $r = f \ (\mathrm{mod}\ g)$

Ideały w pierścieniu $K[x]$

TW. Niech K ciało. Każdy ideał $I \lhd K[x]$ jest równy $I = \langle f \rangle$ dla pewnego $f \in I$

D-d. Niech $I \lhd K[x]$.
Niech $f \in I$ najmniejszego stopnia:
$\forall g \in I \quad st(f) \leq st(g)$

Pokażemy, że $\langle f \rangle \overset{\supsetneq h}{=} I$.
Nie wprost załóżmy, że istnieje $h \notin \langle f \rangle$, $h \in I$.

Z twierdzenia o dzieleniu z resztą istnieją $w, r \in K[x]$ takie że
$$h = f \cdot w + r \quad , \quad st(r) < st(f)$$

Wtedy $r = \underset{\in I}{h} - \underset{\in I}{f} \cdot w \in I$
$st(r) < st(f)$
Sprzeczność bo f najniższego stopnia wśród I
Zatem $\langle f \rangle = I$ $\square$

Przykład: Ideały pierścienia $\mathbb{Z}_5[x]$ to
$\langle 3x^2+1 \rangle$, $\langle x^3+4x+2 \rangle$, ...

- Ideały maksymalne w $K[x]$.

TW. Niech K - ciało, $f \in K[x]$
Ideał $\langle f \rangle$ jest maksymalny $\iff$ f jest wielomianem nierozkładalnym w $K[x]$

D-d.

Założemy nie wprost, że f jest rozkładalny
tzn istnieją $g, h \in K[x]$: $\cdot\ g \cdot h = f$
$\cdot\ st(g), st(h) > 0$

Wtedy $\langle g \rangle \supsetneq \langle f \rangle$ bo $g \in \langle g \rangle \setminus \langle f \rangle$, bo $st\, g < st\, f$
$\langle g \rangle \neq K[x]$ bo $1 \notin \langle g \rangle$.

Zatem $\langle f \rangle$ nie jest ideałem maksymalnym. Sprzeczność.

Założmy że $\langle f \rangle$ nie jest ideałem maksymalnym.

Zatem istnieje $J \triangleleft K[x]$ taki że
$\langle f \rangle \subsetneq J \subsetneq K[x]$

Z poprzedniego twierdzenia istnieje $g \in K[x]$ taki, że
$J = \langle g \rangle$

Mamy więc : $\langle f \rangle \subsetneq \langle g \rangle$, więc $f \in \langle f \rangle$ to $f \in \langle g \rangle$
tzn $g | f$
$st(g) < st(f)$ św. (gdyby to $f | g$)

Więc f jest rozkładalny. □

Przykłady
- W $\mathbb{R}[x]$ ideałem maksymalnym jest $\langle x \rangle, \langle x^2+1 \rangle$
- W $\mathbb{C}[x]$ ideał max : $\langle ix \rangle, \langle ax+b \rangle$
- $\mathbb{Z}_2[x]$ ideał max: $\langle x^3+x+1 \rangle$

Uw. $f = x^3+x+1$ jest nierozkładalny w $\mathbb{Z}_2[x]$, bo,
gdyby być $x^3+x+1 = g(x) \cdot h(x)$ to (bzo) $st(g) = 1$ tzn $g(x) = x + b$,
tzn x^3+x+1 ma pierwiastek $b \in \mathbb{Z}_2$.
Ale $f(0) = 1$, $f(1) = 1$. Sprzeczność, więc f nierozkładalny.

Tw. Niech K - ciało, f wielomian nierozkładalny w $K[x]$.
Wtedy $K[x]/\langle f\rangle$ - ciało.

D-d. Ponieważ f nierozkładalny to $\langle f\rangle$ jest ideałem maksymalnym.

$K[x]$ jest pierścieniem przemiennym z 1.

Więc $K[x]/\langle f\rangle$ jest ciałem. $\square$

Przykład.
Niech $K=\mathbb{Z}_2$, $f=x^3+x+1$. $\langle f\rangle=\{f\cdot w : w\in\mathbb{Z}_2[x]\}$

$\mathbb{Z}_2[x]/\langle f\rangle$ jest ciałem.
Elementy:
$$\mathbb{Z}_2[x]/\langle f\rangle=\{w+\langle f\rangle : w\in\mathbb{Z}_2[x]\}=*$$

[Uw. $w+\langle f\rangle=(w \bmod f)+\langle f\rangle$, bo $w-(w \bmod f)\in\langle f\rangle$]

$*=\{(w \bmod f)+\langle f\rangle : w\in\mathbb{Z}_2[x]\}=\{r+\langle f\rangle : r\in\mathbb{Z}_2[x]\ \mathrm{st}\, r\le 2\}$

Uw $|\mathbb{Z}_2[x]/\langle f\rangle|$ $=\{(ax^2+bx+c)+\langle f\rangle : a,b,c\in\mathbb{Z}_2\}$

dodawanie:
$$(w+\langle f\rangle)+(u+\langle f\rangle)=(w+u)+\langle f\rangle=w\underset{f}{+}u+\langle f\rangle$$
mnożenie:
$$(w+\langle f\rangle)\cdot(u+\langle f\rangle)=(w\cdot u)+\langle f\rangle=[(w\cdot u) \bmod f]+\langle f\rangle=w\underset{f}{\cdot}u+\langle f\rangle$$

Ciało generowane przez wielomian nierozkładalny $f \in K[x]$

Elementy ciała $\{ r \in K[x] : \text{st } r < \text{st } f \}$

dodawanie : $w +_f u = w + u$.

mnożenie $w \cdot_f u = w \cdot u \pmod{f}$.

Uwaga. Moc ciała jest równa $|K|^{st(f)}$.