26. Полиноми на една променлива. Теорема за деление с остатък. Най-голям общ делител на полиноми – тъждество на Безу и алгоритъм на Евклид. Зависимост между корени и коефициенти на полиноми (формули на Виет).

Анотация: Във въпроса се включва определение на полином с коефициенти над поле, степен на полином и корени на полиноми. Теорема за деление с остатък. Схема на Хорнер. Всеки идеал във F[x] е главен. Принцип за сравняване на коефициенти. Определение на най-голям общ делител на два полинома НОД $\big(h(x),\, g(x)\big) = \big(h(x),\, g(x)\big)$, теорема за съществуване на най-голям общ делител на два полинома с коефициенти над поле, изразяване на $\big(h(x),\, g(x)\big)$ чрез полиномите $h(x)$ и $g(x)$ (тъждество на Безу), алгоритъм на Евклид. Корени на полиноми. Формули на Виет за полином от степен n с коефициенти от поле.

Дефиниция (полином с коефициенти над поле). Нека F е произволно поле. Дефинираме множеството $F[x] = \{f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \,|\, a_i \in F\}$, т.е. $F[x]$ съдържа тези безкрайни редици, които имат краен брой ненулеви елементи от F. Елементите (редиците) на така дефинираното множество $F[x]$ ще наричаме полиноми.
Нека $f = (a_0, a_1, \ldots, a_n, \ldots) \in F[x]$ и $g = (b_0, b_1, \ldots, b_n, \ldots) \in F[x]$. Въвеждаме следните две бинарни операции във $F[x]$:
а) Събиране: $f + g = (a_0 + b_1, a_1 + b_1, \ldots, a_n + b_n, \ldots) \in F[x]$;
б) Умножение: $f \times g = (c_0, c_1, \ldots, c_n, \ldots) \in F[x]$, където $c_k = \sum_{k=i+j} a_i b_j$.
Така дефинираното $F[x]$ директно се проверява, че е комутативен пръстен с 1-ца.

Наричаме $F[x]$ пръстен на полиномите на една променлива x с коефициенти от полето F. Казваме, че $f = g \Leftrightarrow a_i = b_i,\ \forall i \in \mathbb{N}_0$.

Съществува биекция, която изпраща $a \in F$ в редицата $(a, 0, 0, \ldots) \in F[x]$. Нека означим $x = (0, 1, 0, \ldots)$. Тогава при така дефинираните операции във $F[x]$ лесно се вижда, че $x^n = (0, 0, \ldots, 0, 1, 0, \ldots)$, където 1 се намира на $n+1^{\text{-вата}}$ позиция, като броенето започва от 1. Също се вижда, че $ax = (a, 0, 0, \ldots)(0, 1, 0, \ldots) = (0, a, 0, \ldots)$. Така получаваме, че всеки полином $f \in F[x]$ може да се представи по следния единствен начин: $f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, където a_n е последният ненулев елемент от редицата. Така получаваме още един еквивалентен начин, по който може да дефинираме $F[x]$:

$$F[x] = \{f = a_0 + a_1 x + \ldots + a_n x^n \,|\, a_i \in F,\ \forall i = \overline{0, n} \text{ и } \forall n \in \mathbb{N}\}.$$

Нека имаме $f \in F[x]$ и $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, където a_n е последният ненулев коефициент. Коефициентите на f съответно наричаме: a_n – старши коефициент, a_i – коефициенти, a_0 – свободен коефициент. Числото n наричаме степен на f и означаваме $\deg(f) = n$. Полиномите от нулева степен наричаме константни полиноми. Те са от вида $f = a \in F[x]$. По дефиниция нулевият полином има степен $\deg(0) = -\infty$.

Дефиниция (делители на нулата). Нека M е пръстен и $a, b \in M,\ a \neq 0,\ b \neq 0,\ ab = 0$. Тогава наричаме a и b делители на нулата в пръстена M.
Ако M е комутативен пръстен с 1-ца и няма делители на нулата, то M е област.

Забележка. Всяко поле е област, но не всяка област е поле.

Дефиниция (степен на полином). Степента на един полином на една променлива е равна на най-високата степен на променлива с ненулев коефициент. За степените на полиномите (f и g) от $F[x]$ са в сила следните две свойства:

а) $\deg(f+g) \leq \max\big(\deg(f),\ \deg(g)\big)$;

б) Ако F е област, то $\deg(fg) = \deg(f) + \deg(g)$ и $F[x]$ също е област.

Дефиниция (корен на полином). Нека $f \in F[x]$, $\deg(f) > 0$ и K е разширение на F, $\alpha \in K$. Казваме, че α е корен на f, ако за $f(x) \in K[x]$ е в сила $f(\alpha) = 0$.

Теорема 1 (деление с частно и остатък). Нека F е поле. Нека $f, g \in F[x]$, $g \neq 0$. Тогава съществуват единствени $q, r \in F[x]$ такива, че $f = q \times g + r$, $\deg(r) < \deg(g)$. Казваме, че q е частно, а r – остатък при деление на f с g.

Доказателство:

Съществуване. Нека $\deg(f) = n$, $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $a_0 \neq 0$ и $\deg(g) = m$, $g = b_0x^m + b_1x^{m-1} + \ldots + b_m$, $b_0 \neq 0$. Ще направим доказателство с индукция по n.

1) $\deg(f) < \deg(g)$. Тогава $f = 0 \times g + f \Rightarrow q = 0$ и $r = f$.
   Тогава $\deg(r) = \deg(f) < \deg(g)$.
2) $\deg(g) = 0 \Rightarrow g = a \in F$. Тогава $f = g \times \frac{f}{g} = g \times \frac{f}{a}$ и следователно $q = \frac{f}{a}$ и $r = 0$.
   Така отново $\deg(r) < \deg(g)$.
3) $\deg(f) > \deg(g)$ и $\deg(g) = m \neq 0$. Да разгледаме $Q = \frac{a_0}{b_0} \times x^{n-m}$. Ако вземем $Q \times g$, то това е полином със старши член a_0x^n, т.е. съвпада със старшия член на f.
   Сега нека $f_1 = f - Q \times g$. Следователно за построения f_1 е вярно, че $\deg(f_1) < \deg(f) = n$. Съгласно индукционното предположение, веки полином от степен строго по-малка от n може да се представи във вида $f' = q' \times g + r'$, за някакви $q', r' \in F[x]$, такива, че $\deg(r') < \deg(g)$. Тогава $f_1 = q_1 \times g + r_1$. Сега можем да заместим: $f = f_1 - Q \times g = q_1 \times g - Q \times g + r_1 = (q_1 - Q) \times g + r_1$ и сега след полагане $q = q_1 - Q$ и $r = r_1$ получаваме, че $f = q \times g + r$, където $\deg(r) = \deg(r') < \deg(g)$. Така покачваме, че q и $r \in F[x]$ съществуват.

Единственост. Нека $f = q_1 \times g + r_1 = q_2 \times g + r_2$. Нека $q_1 \neq q_2$ и $r_1 \neq r_2$. Тогава $(q_1 - q_2) \times g = r_2 - r_1$.

$\deg\big((q_1 - q_2) \times g\big) = \deg\big(q_1 - q_2\big) + \deg\big(g\big) \geq \deg(g)$.

$\deg(r_2 - r_1) \leq \deg(r_2) < \deg(g)$ по условие.

$\Rightarrow \deg\big((q_1 - q_2) \times g\big) > \deg(r_2 - r_1)$, което е противоречие.

□

Схема на Хорнер. Тя е директно следствие от теорема 1. Нека $f \in F[x]$, $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $a_0 \neq 0$. $g = (x - \alpha) \in F[x]$. Съгласно теорема 1, $f = q \times g + r$ и $\deg(r) < \deg(g) = \deg(x - \alpha) = 1 \Rightarrow r = a$ – константа, $r \in F$ и q има вида $q = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}$. Схемата на Хорнер помага за намирането на корени на полиноми – ако $r = 0$, казваме, че α е корен. Така представяме f по следния начин:

$f = (x - \alpha)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + r = a_0^n + a_1x^{n-1} + \ldots + a_n$.

Коефициентите на q и r намираме като разкрием скобите и директно сравним коефициентите пред различните степени на x. Така ще видим, че:

$$\begin{aligned} b_0 &= a_0 \\ b_1 &= a_1 + \alpha b_0 \\ b_2 &= a_2 + \alpha b_1 \\ &\cdots \\ b_i &= a_i + \alpha b_{i-1} \\ &\cdots \\ b_{n-1} &= a_{n-1} + \alpha b_{n-2} \\ r &= a_n + \alpha b_{n-1} \end{aligned}$$

Дефиниция (идеал). Нека F е пръстен. Нека $I \neq \emptyset$ и $I \subseteq F$. Казваме, че I е идеал (двустранен идеал) на F и означаваме $I \trianglelefteq F$ или $I \triangleleft F$, ако I се съдържа строго във F, ако е в сила, че:

а) ако $a, b \in I$, то $a - b = a + (-b) \in I$;

б) ако $a \in I, r \in F$, то $ra = ar \in I$.

Забележка. Ако от второто условие само $ra \in I$, казваме, че I е ляв идеал, а ако само $ar \in I$, казваме, че I е десен идеал.

Ако съществува $a \in I$ такова, че $I = <a> = \{ar \mid r \in F\}$, казваме, че I е главен идеал, породен от елемента a.

Теорема (всеки идеал във $\mathbf{F[x]}$ е главен). Нека F е поле. Тогава всеки идеал I във $F[x]$ е главен идеал.

Доказателство:

Нека $I = \{0\}$. Тогава е ясно, че I е главен идеал. Нека $I \neq \{0\}$. Тогава нека вземем ненулев полином g, който е от минимална степен от I. Ще докажем, че $<g> = I$.

1) $I \subseteq <g>$. Нека вземем произволен полином $f \in I$. Съгласно Теорема 1, можем да представим f по следния начин: $f = q \times g + r$, където $\deg(\mathrm{r}) < \deg(\mathrm{g})$. Но това означава, че $r = f - q \times g$ и $r \in I$. Нека $r \neq 0 \Rightarrow$ Получаваме противоречие с избора на g да бъде от минимална степен от I, тъй като получихме, че $\deg(r) < \deg(g)$. Следователно $r = 0$. Така $f = g \times q \in <g>$, $\forall f \in I$ и следователно $I \subseteq <g>$.
2) $<g> \subseteq I$. Нека вземем произволно $s \in <g>$. Тогава $s = q \times g$, където $g \in I \Rightarrow s \in I$.

От 1) и 2) $\Rightarrow I = <g>$.

□

Следствие 1. Нека K е комутативен пръстен с 1, $f \in K[x]$, $\deg(f) > 0$, $\alpha \in K$. Тогава $f(\alpha) = 0 \Leftrightarrow f = (x - \alpha)q$ за някое $q \in K[x]$.

Доказателство: От теорема 1 следва, че $f = \underbrace{(x - \alpha)}_{g} \times q + r$, $\deg(r) < \deg(g) = 1 \Rightarrow r$ е константа. Заместваме x с α и получаваме, че α е корен на $f \Leftrightarrow f(\alpha) = 0 \Leftrightarrow r = 0 \Leftrightarrow f = (x - \alpha) \times q$ за някое $q \in K[x]$.

Следствие 2. Нека K е област и $f \in K[x]$, $\deg(f) = n > 0$ и съществуват два по два различни елемента от K : $\alpha_1, \ldots, \alpha_{n+1}$. Ако $f(\alpha_i) = 0$, $\forall i = n + 1$, то f е нулевия полином – $f = 0$. Т.е. полином от степен не по-голяма от n не може да има повече от n два по два различни корени.

Доказателство: Допускаме, че $f \neq 0$. Нека $f(\alpha_1) = 0$. Тогава съгласно следствие 1, $f = (x - \alpha_1) \times q_1$, където $q_1 \in K[x]$. Същевременно $f(\alpha_2) = 0$ и следователно $(\alpha_2 - \alpha_1) \times q_1(\alpha_2) = 0$, но $\alpha_2 - \alpha_1 \neq 0$ по условие и нямаме делители на нулата. Следователно $q_1(\alpha_2) = 0$, но така по следствие 1 $\Rightarrow q_1 = (x - \alpha_2) \times q_2$, за $q_2 \in K[x]$. Така $f = (x - \alpha_1)(x - \alpha_2) \times q_2$. Сега можем да използваме, че $f(\alpha_3) = 0$ и следователно $q_2(\alpha_3) = 0$ и т.н. Така след $n + 1$ стъпки стигаме до $f = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{n+1}) f_{n+1}$. Нека $f_{n+1} \neq 0 \Rightarrow \deg(f_n) \geq 0$. Тогава обаче получаваме, че $\deg(f) \geq n + 1$, което е противоречие. По условие $\deg(g) = n < n + 1$, следователно $f = 0$. С това следствието е доказано.

Теорема 2 (принцип за сравняване на коефициенти). Нека F е област. Нека $g_1, g_2 \in F[x]$ и $\deg(g_1) \leq n$, $\deg(g_2) \leq n$. Нека съществуват $n + 1$ два по два различни елемента $\alpha_1, \ldots, \alpha_{n+1}$ от F такива, че $g_1(\alpha_i) = g_2(\alpha_i)$ за $i = \overline{1, n+1}$. Тогава $g_1 = g_2$.

Доказателство: Нека $f = g_2 - g_1$. Тогава $\exists n + 1$ два по два различни елемента на F: $\alpha_1, \ldots, \alpha_{n+1}$, за които $f(\alpha_i) = 0$, $\forall i = \overline{1, n+1}$ и $\deg(f) \leq \max(g_2, g_1) \leq n$. Следователно от следствие 2 получаваме, че f е нулевия полином $f = 0$ и следователно $g_1 - g_2 = 0 \Leftrightarrow g_1 = g_2$. С това принципът за сравняване на коефициенти е доказан.

□

Дефиниция (делимост). Нека F е поле. Нека $f, g \in F[x]$, $g \neq 0$. Казваме, че g дели f и пишем $g \mid f$, ако $\exists$ полином $q \in F[x] : f = q \times g$. В противен случай казваме, че g не дели f или пишем $g \nmid f$.

Свойства на делимост на полиноми:

1) Всеки полином дели себе си . Нещо повече, $\forall a, b \in F : af \mid bf, a \neq 0$;
2) Ако $g \mid f$, то $\forall a, b \in F, a \neq 0 : ag \mid bf$;
3) Ако $g \mid f$ и $f \mid h$, то $g \mid h$;
4) Ако $g \mid f$ и $f \mid g$, то $g = af$, където a е константа. В частност, ако $g \mid f$ и $f \mid g$ и старшите коефициенти на g и f съвпадат, то $g = f$;
5) Ако $g \mid h_1, h_2, \ldots, h_k$, то $g \mid (h_1 t_1 + \ldots + h_k t_k) \forall t_i \in F[x], i = \overline{1,k}$;
6) Ако $g \mid f_1 + f_2$ и $g \mid f_1$, то $g \mid f_2$. В частност, ако $f_1 + f_2 = 0$ и $g \mid f_2$, то $g \mid f_1$.

Дефиниция (НОД). Нека F е поле. Нека $f, g \in F[x]$, $g \neq 0$. Най-голям общ делител (НОД) на полиномите f и g наричаме полинома $d(x) \in F[x]$, за който е изпълнено, че:
1) $d \mid f, d \mid g$
2) Ако $d_1 \mid f$ и $d_1 \mid g$, то $d_1 \mid d$.
В този случай казваме, че d е НОД на f и g и означаваме $d = (f, g)$.

НОД се определя с точност до ненулева константа. Това означава, че ако $d = (f, g)$ и $a \in F$, то $ad = (f, g)$, за $a \neq 0$. Ако старшият коефициент на d е 1, то d е еднозначно определен.

Дефиниция (взаимно прости полиноми). Казваме, че полиномите f и g са взаимно прости, ако $(f, g) = a$ – константа. Тогава може да считаме, че $(f, g) = 1 = d$.

Аналогично (рекурсивно) дефинираме НОД за повече от два полинома.

Твърдение (∃ НОД). Всеки два полинома $f, g \in F[x], g \neq 0$ притежават НОД.

Доказателство: Нека I е идеалът на пръстена $F[x]$, породен от f и g. Тоест $I = \{uf + vg \mid u, v \in F[x]\}$. По условие $g \neq 0 \Rightarrow I \neq \{0\}$. Вече показахме, че в полето $F[x]$ всички идеали са главни. Следователно $I = <d>$. Ще покажем, че $d = (f, g)$.

1) $f, g \in I \Rightarrow f = f_1 \times d, g = g_1 \times d$ за някакви $f_1, g_1 \in F[x]$. Това обаче означава, че $d \mid f$ и $d \mid g$.
2) $d \in I \Rightarrow d = uf + vg$ за някакви $u, v \in F[x]$. Сега нека $d_1 \mid f$ и $d_1 \mid g$. Тогава от свойство 5 следва, че $d_1 \mid uf + vg$ за всякакви $u, v \in F[x]$. Следователно $d_1 \mid d$.

От 1) и 2) следва, че d е НОД на f и g, т.е. $d = (f, g)$.

□

В това доказателство показахме т.нар. **тъждество на Безу**. Нека $f, g \in F[x], g \neq 0$. Тогава $\exists u, v \in F[x]$ такива, че $uf + vg = d$, където $d = (f, g)$. В частност, ако f, g са взаимно прости, то $uf + vg = 1 = d$. Вярно е и обратното – ако съществуват u и v такива, че $uf + vg = 1$, то f и g са взаимно прости.

Друго доказателство за съществуването на НОД за всеки $f, g \in F[x], g \neq 0$ е чрез **алгоритъма на Евклид**. Алгоритъмът на Евклид гласи следното – взимайки двете дадени на входа на алгоритъма числа a и b, проверяваме дали b е равно на 0. Ако да, числото a е търсеният най-голям общ делител. Ако не, повтаряме процеса, като използваме за входни данни b и остатъка, получен при деленето a на b (означаван по-долу с $a \mod b$). Аналогично може да приложим този алгоритъм и за полиноми, вместо числа.

Теорема 1 ни позволява да изразим последователно:

$$f = q_1 g + r_1, \ \deg(r_1) < \deg(g) \qquad (1)$$
$$g = q_2 r_1 + r_2, \ \deg(r_2) < \deg(r_1) \qquad (2)$$
$$r_1 = q_3 r_2 + r_3, \ \deg(r_3) < \deg(r_2) \qquad (3)$$

и т.н.

Правилото, което следваме е, че делим „всеки получен остатък на следващия“, докато не получим нулев остатък. Тъй като степените на остатъците, които получаваме строго намаляват, то рано или късно ще получим нулев остатък.

Нека б.о.о. $r_4 = 0$. Това очзначава, че $r_2 = q_4 r_3$ (4).

Ще покажем, че последният ненулев остатък е търсеното d. (Ако още $f = q \times g$, то $d = g$)

От 4) следва, че $r_3 \mid r_2$. Сега може да заместим израза за r_2 в 3) и ще получим, че $r_3 \mid r_1$. Аналогично $r_3 \mid g$ и $r_3 \mid f \Rightarrow$ отговаря на условие 1) за d.

Нека сега $d_1 \mid f$ и $d_1 \mid g$. От 1) следва, че $r_1 = f - q_1 \times g \Rightarrow d_1 \mid r_1$. Аналогично $d_1 \mid r_2$ и $d_1 \mid r_3 \Rightarrow r_3$ отговаря и на условие 2) за d. Така показахме, че r_3 е търсеното от нас $d = (f, g)$.

□

Корени на полиноми

Дефиниция (k-кратен корен). Нека $f \in F[x], \deg(f) > 0, \alpha \in K, K$ е разширение на F. Казваме, че α е k-кратен корен $(k \geq 1)$ на f, ако $f = (x - \alpha)^k g$, за някое $g \in F[x]$ и $g \neq 0$. Ако $k = 1$ ще казваме, че k е прост корен. Ако $k \geq 1$ ще казваме, че k е кратен корен.

Теорема. Нека F е поле, $f \in F[x]$ и $\deg(f) > 0$. Тогава съществува разширение $K \geq F$, в което полиномът f има корен.

Твърдение. Нека F е поле, $f \in F[x]$ и $\deg(f) = n > 0$. Тогава съществува разширение L на полето F, над което f се разлага в произведение на линейни множители: $f = a_0(x - \alpha_1)\dots(x - \alpha_n)$, т.е. всички корени на f са в това разширение.

Доказателство:
Нека K_1 е разширение на F, в което f има корен α_1. Тогава $f(\alpha_1) = 0$ и съгласно следствие 1 имаме, че $f = (x - \alpha_1)f_1$, $f_1 \in K_1[x]$, $\deg(f_1) = n - 1$. Ако $\deg(f_1) > 0$, то нека K_2 е разширение на K_1, в което f има корен α_2. От следствие 1 $\Rightarrow f_1 = (x - \alpha_2)f_2, f_2 \in K_2[x]$, $\deg(f_2) = n - 2$. Може да заместим в f и да получим, че $f = (x - \alpha_1)(x - \alpha_2)f_2$. Продължаваме по същия начин и след n направени стъпки ще получим:
$f = (x - \alpha_1)\dots(x - \alpha_n)f_n, f_b \in K_n$ и $L = K_n$. Тогава $\alpha_1, \dots, \alpha_n$ са всичките корени на f, а $f_n = a_0$ е старшият коефициент на f.

□

Дефиниция (поле на разлагане). Нека F е поле, $f \in F[x]$, $\deg(f) = n > 0$. Най-малкото поле L, което е разширение на F и съдържа всички корени $\alpha_1, \dots, \alpha_n$ се нарича поле на разлагане на полинома f над полето F.

Формули на Виет. Нека F е поле, $f \in F[x]$, $\deg(f) = n > 0$. Нека $L \geq F$ е поле на разлагане на $f(x)$ над полето F. Може да представим f по следните два начина:

$$f = a_0(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n) = a_0\prod_{i=1}^{n}(x - \alpha_i) = a_0x^n + a_1x^{n-1} + \dots + a_n = \sum_{i=0}^{n} a_ix^{n-i},$$

$a_0 \neq 0$. Ако разкрием скобите и сравним директно коефициентите пред различните степени на x отляво и отдясно, то ще получим зависимости между корените $\alpha_1, \dots, \alpha_n$ на f и коефициентите му пред различните степени на x. Тези зависимости са известни като формули на Виет:

$$\begin{aligned}
\alpha_1 + \alpha_2 + \dots + \alpha_n &= -\frac{a_1}{a_0} \\
\alpha_1\alpha_2 + \alpha_2\alpha_3 + \dots + \alpha_{n-1}\alpha_n &= \frac{a_2}{a_0} \\
&\dots \\
\alpha_1\alpha_2\dots\alpha_i + \dots + \alpha_{n-i+1}\dots\alpha_{n-1}\alpha_n &= (-1)^i\frac{a_i}{a_0} \\
&\dots \\
\alpha_1\alpha_2\dots\alpha_n &= (-1)^n\frac{a_n}{a_0}
\end{aligned}$$

Общо формулите на Виет могат да се представят като

$$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k} = (-1)^k\frac{a_k}{a_0},$$

където броят на събираемите в сумата k идва от биномния коефициент $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Тук ще дефинираме няколко понятия, които използвахме „наготово“ в изложението.

Дефиниция (пръстен). Нека R е непразно множество, в което са дефинирани операциите събиране и изваждане. Казваме, че R е пръстен, ако R е комутативна група относно операцията събиране (неутралният елемент относно събиране наричаме нулев елемент или само нула) и в допълнение $\forall a, b, c \in R$ е в сила:
1) $a(bc) = (ab)c$ – асоциативен закон;
2) $a(b + c) = ab + ac, (a + b)c = ac + bc$ – дистрибутивни закони.

(1) Пръстен с 1-ца. Казваме, че пръстена R е пръстен с 1 (единица), ако в R съществува неутрален относно умножението елемент.

(2) Комутативен пръстен. Казваме, че пръстена R е комутативен, ако $\forall a, b \in R$ е в сила $ab = ba$.

Комутативен пръстен с 1. Казваме, че пръстена R е комутативен с 1, ако едновременно са в сила условия (1) и (2) от по-горе.

Дефиниция (поле). Поле наричаме комутативен пръстен с 1, в който всеки ненулев елемент е обратим.

Всяко поле е област. Нека F е поле и $a, b \in F, a \neq 0$. Тогава, ако $ab = 0$ и умножим с a^{-1}, получаваме $b = 0$. Обратното не е вярно. Не всяка област е поле.

Подполе / разширение на поле. Нека F е поле и K е непразно подмножество на F съдържащо поне два елемента. Казваме, че K е подполе на F, ако от това, че $a, b \in K$ следва, че $a + b, a - b, ab, a^{-1} \in K$. Тогава в K се съдържат и 0 и 1 и следователно K също е поле. Ако K е подполе на F, то казваме, още че F е разширение на K и пишем $F \geq K$ или $F > K$, ако F строго съдържа K (K строго се съдържа във F).