Аритметика в пръстена на полиномите над поле.

Разглеждаме пръстена на полиномите $F[x]$ с коефициенти от поле F. Нека $f, g \in F[x]$ са такива, че $g \neq 0$. Казваме, че g *дели* f, ако съществува полином $q \in F[x]$, такъв че $f = qg$ или с други думи, при деление на f на g с частно q и остатък r е изпълнено, че $r = 0$. Означаваме $g \mid f$. Ако g не дели f, пишем $g \nmid f$.

Свойства:

1. Ако $g \mid f$, то $bg \mid af$ за $\forall a, b \in F, b \neq 0$. Наистина $f = qg$ за полином $q \in F[x]$ и сега за $a, b \in F$ имаме, че $af = qagbb^{-1}$.

2. Ако $g \mid f$ и $f \mid g$, то $f = cg$ за $c \in F, c \neq 0_F$. Наистина, щом $g \mid f$, то $\exists q \in F[x] : f = qg$. От друга страна $f \mid g$, откъдето $\exists q_1 \in F[x] : g = q_1 f$. Замествайки последното в равенството $f = qg$, получаваме $f = qq_1 f$. Това означава, че $\deg(qq_1) = 0$, т.е. $qq_1 \in F$. Оттук следва, че или $\deg q = 0$, или $\deg q_1 = 0$. И в двата случая получаваме, че $\deg f = \deg g$, което пък влече, че $\deg q = 0$, т.е. $q \in F\{0_F\}$ и след полагане $c = q \in F$ получаваме $f = cg$. Това свойство може да бъде изказано така: ако два полинома взеимно се делят, то те съвпадат с точност до ненулева константа от полето F.

3. Ако $g \mid f$ и $f \mid h$, то $g \mid h$.

4. Ако g дели $f_1, f_2, \ldots, f_k$, то g дели и $t_1 f_1 + t_2 f_2 + \cdots + t_k f_k$ за произволни $t_i \in F[x], i = 1, 2, \ldots, k$.

Нека $f, g \in F[x] \backslash \{0\}$. Полиномът $d \in F[x]$ се нарича *най-голям общ делител (НОД) на f и g*, ако $d \mid f$ и $d \mid g$ и ако $d_1 \in F[x]$ е такъв, че $d_1 \mid f$ и $d_1 \mid g$, то $d_1 \mid d$. В частност това означава, че $\deg d \geq \deg d_1$, т.е. най-големият общ-делител е полином от най-висока степен измежду всички

общи делители на f и g. Ако d и d' са НОД на f и g, то по дефиниция имаме, че $d \mid d'$ и $d' \mid d$, което означава, че $d = cd'$ за $c \in F\backslash\{0\}$. За да постигнем еднозначност, считаме, че НОД е полином d със стрши коефициент 1, т.е. d е *унитарен полином*. По този начин d е единственият НОД на f и g и пишем $d = (f, g)$. Строго доказателство дава следното

Твърдение 1. *Съществува единствен НОД на* $f, g \in F[x]$.

Доказателство. Разглеждаме множеството

$$I = \{uf + vg \mid u, v \in F[x]\} \subseteq F[x].$$

За два произволни елемента от I имаме, че $(u_1 f + v_1 g) - (u_2 f + v_2 g) = (u_1 - u_2)f + (v_1 - v_2)g \in I$, а за произволен елемент от I и прозиволен полином $h \in F[x]$ имаме, че $h(uf + vg) = (hu)f + (hv)g \in I$. Това доказва, че $I \trianglelefteq F[x]$ е идеал в полиномиалния пръстен. Т.к всеки идеал на $F[x]$ е главен, то $\exists d \in F[x]$, такъв че $I = (d)$ и d е ненулев полином от насйниска степен, принадлежащ на I. Очевидно $f \in I$ при $u = 1_F$ и $v = 0_F$ и $g \in I$ при $u = 0_F$ и $v = 1_F$. Сега това значи, че $f, g \in (d)$ и $d \mid f$ и $d \mid g$. От друга страна $d \in (d)$ дава $d \in I$ и $d = uf + vg$ за някакви полиноми $u, v \in F[x]$. Ако $d_1 \in F[x]$ е такъв, че $d_1 \mid f$ и $d_1 \mid g$, то тогава според свойство 4 $d_1 \mid uf + vg$, т.е. $d_1 \mid d$. Всичко това означава, че $d = (f, g)$. Единствеността следва от уговорката d да бъде избран така, че старшият му коефициент да е равен на 1_F. □

Едновременно с това твърдение доказахме и тъждеството на Безу за полиноми, а именно, че ако $f, g \in F[x]$ и $d \in F[x]$ е такъв, че $d = (f, g)$, то $\exists u, v \in F[x] : d = uf + vg$.

Продължавайки аналогията с пръстена на целите числа ще изложим алгоритъма на Евклид за намиране на НОД. Нека $f, g \in F[x]$. Ако $g \mid f$, то просто полагаме $d = g$. Нека $d \nmid f$. Според теоремата за деление на полиноми получаваме, че

$$f = qg + r$$

за подходящи полиноми $q, r \in F[x]$ като $\deg r < \deg g$. Сега делим с частно q_1 и остатък r_1 полиномът g на остатъка r и получаваме

$$g = q_1 r + r_1$$

като отново $\deg r_1 < \deg r$. Продължавайки по същия начин, делейки всеки остатък r_i на следващия r_{i+1} получаваме поредицата от равенства

$$r = q_2 r_1 + r_2, \quad \deg r_2 < \deg r_1,$$

...

$$r_{k-2} = q_k r_{k-1} + r_k, \quad \deg r_k < \deg r_{k-1},$$

$$r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad \deg r_{k+1} < \deg r_k.$$

Така редицата $\deg g > \deg r > \deg r_1 > \ldots$ не може да е безкрайна, защото е строго намалява редица от неотрицателни цели числа. По този начин се оказва, че някой пореден остатък е нулевият полином. Нека $k \geq 0$ е най-малкото цяло число, съсвойството $r_{k+1} = 0$, т.е. $r_{k-1} = q_{k+1} r_k$. Ще докажем, че търсеният НОД е $d = r_k$. Наистина, проследявайки обратния ход на алгоритъма виждаме, че r_k дели $r_{k-1}, r_{k-2}, \ldots, r_2, r_1, r, g$ и f. Нека $d_1 \in F[x]$ е такъв, че $d_1 \mid f$ и $d_1 \mid g$. Тогава, движейки се по правия ход на алгоритъма, виждаме, че d_1 дели $f, g, r, r_1, \ldots, r_{k-2}, r_{k-1}$ и $r_k = d$. Така се оказва, че $d = (f, g)$.

Ще казваме, че полиномите f и g са *взаимно прости*, ако $(f, g) = 1_F$ или $(f, g) = c \in F$, когато не сме изискали единствеността на НОД с уговорката, той да бъде избран като унитарен полином.

Свойства:

5. Ако $d = (f, g)$ и $f = df_1, g = dg_1$, за $f_1, g_1 \in F[x]$, то $(f_1, g_1) = 1_F$. Наистина, тъждеството на Безу ни дава, че съществуват полиноми $u, v \in F[x]$, такива че $uf + vg = d$. Заместваики изразите за f и g в него, получаваме $udf_1 + vdg_1 = d$. Сега след като разделим двете страни на равенството на d имаме $uf_1 + vg_1 = 1_F$, което означава, че $(f_1, g_1) = 1_F$.

6. Ако $g \mid f_1 f_2$ и $(g, f_1) = 1_F$, то $g \mid f_2$. Наистина, $(g, f_1) = 1_F$ означава, че същесвуват полиноми u, v, такива че $ug + vf_1 = 1_F$. След умножение на двете страни с f_2 получаваме еквивалентното неравенство $ugf_2 + vf_1 f_2 = f_2$. Сега, понеже $g \mid g$ и $g \mid f_1 f_2$, то g дели цялата лява страна, а оттам следва, че трябва да дели и дясната, т.е. изпълнено е $d \mid f_2$.

Нека $f \in F[x]$ и $\deg f \geq 1$. Казваме, че f е *неразложим над* F, ако f няма други делители в $F[x]$ освен c и cf, където $c \in F \backslash \{0_F\}$ е ненулева константа. Еквивалентна дефиниция на същото понятие е f да не може да се представи като произведение на полиноми във вида $d = gh$ за $g, h \in F[x]$ с $\deg g > 0$ и $\deg h > 0$.

Важно е да споменаваме полето, над което даден полином е неразложим, защото е възможно този въпрос да има различен отговор спрямо

различните полета. Полиномът $f(x) = x^2 - 2$ например може да се разглежда както като полином с цели коефициенти $f \in \mathbb{Z}[x]$, така и в качеството си на полином с реални коефициенти $f \in \mathbb{R}[x]$. Полиномът F обаче е неразложим над $\mathbb{Q}$, понеже уравнението $x^2 = 2$ няма рационални корени. В другия случай обаче имаме, че $\sqrt{2} \in \mathbb{R}$ и в такъв случай може да запишем $f(x) = (x-\sqrt{2})(x+\sqrt{2})$, което означава, че f е разложим над $\mathbb{R}$.

Свойства:

7. Ако $f \in F[x]$ е прозиволен полином, а $g \in F[x]$ е неразложим над F, то или $g \mid f$, или $(g, f) = 1_F$. Наистина, нека $d = (g, f)$. Ако $d = 1_F$, то няма какво да доказваме. Нека сега $d \neq 1_F$. Имаме, че $d \mid g$, но т.к. g е неразложим, то трябва $d = cg$ за $c \in F\backslash\{0_F\}$. Оттук веднага следва, че $g \mid f$.

8. Ако g е неразложим над F и $g \mid f_1 f_2$, то или $g \mid f_1$, или $g \mid f_2$. Наистина, ако $g \mid f_1$, то всичко е наред. Нека сега $g \nmid f_1$. Тогава $(g, f_1) = 1_F$ и $g \mid f_1 f_2$ в комбинация със свойство 6 дават $g \mid f_2$.

9. Ако $g_1 \mid f, g_2 \mid f$ и $(g_1, g_2) = 1_F$, то $g_1 g_2 \mid f$. Наистина, при тези условия $f = qg_1$ за подходящ полином $g \in F[x]$. Тогава $g_2 \mid qg_1$ и според свойство 6 $g_2 \mid q$. Това означава, че $q = tg_2$ за някакъв полином $t \in F[x]$ и по този начин $f = g_1 g_2 t$. Оттук е очевидно, че свойството е в сила.

Продължаваме с аналога на основната теорема на аритметиката в полиномиалния пръстен над поле F.

Теорема. *Всеки полином f с коефициенти от поле F и степен $\deg f \geq 1$ се разлага в произведение на неразложими над F полиноми. Ако $f = p_1 \dots p_r$ и $f = q_1 \dots q_s$ са две такива разлагания, то $r = s$ и $q_i = c_i p_i$, където $c_i \in F\backslash\{0_F\}$ за $\forall i = 1, 2, \dots, r$, т.е. това разлагане е единствено с точност до константен ненулев множител от полето F.*

Доказателство. Съществуване: ако f е неразложим над F, то той очевидно няма нужда от допълнително разлагане. Провеждаме доказателството с индукция по степента на полинома f. Основа на индукцията – $\deg f = 1$. В този случай f е неразложим и всичко е изпълнено. Индукционно предположение – нека $\deg f \geq 2$ и твърдението е изпълнено за всички полиноми от степен по-малка от $\deg f$. Индукционна стъпка – може да считаме, че $f = gh$ за полиноми $g, h \in F[x]$ с $\deg g < \deg f$ и $\deg h < \deg f$. Индуктивно, g и h се разлагат в произведение на нераз-

ложими полиноми и тогава $f = gh$ също се разлага в произведение на неразложими полиноми.

Единственост: нека $f = p_1 p_2 \dots p_r$ и $f = q_1 q_2 \dots q_s$, където $r, s \geq 1$ са две разлагания в неразложимите над F полиноми p_i, q_j, $i = 1, \dots, r, j = 1, \dots, s$. Тогава имаме, че

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Нека за определеност $r \leq s$. От равенството следва, че $p_1 \mid q_1 q_2 \dots q_s$ и понеже p_1 е неразложим, то p_1 дели поне един от полиномите $q_1, q,2, \dots, q_s$. Нека след евентуално преномериране на индексите считаме, че $p_1 \mid q_1$. Т.к. имаме, че q_1 също е неразложим, то получаваме, че $q_1 = c_1 p_1$ за ненулев елемент от полето от константи $c_1 \in F \backslash \{0_F\}$. Дотук получихме, че

$$p_1 p_2 \dots p_r = c_1 p_1 q_2 \dots q_s$$

и след като разделим двете страни на p_1 имаме, че

$$p_2 \dots p_r = c_1 q_2 \dots q_s.$$

Продължавайки по същия начин след r на бройстъпки достигаме до $q_i = c_i p_i$ за $c_i \in F \backslash \{0_F\}$, $i = 1, \dots, r$ и равенството

$$1_F = c_1 c_2 \dots c_r q_{r+1} \dots q_s.$$

Ако допуснем, че $s > r$, то $0 = \deg 1_F = \deg q_{r+1} + \dots + \deg q_s > 0$, което е противоречие. Следователно $s = r$ и $q_i = c_i p_i$ за $i = 1, 2, \dots, r$, което всъщност твърдеше теоремата. $\square$