Глава 11

Въпрос 11: Еднозначно разлагане на полиноми в произведение от неразложими множители

Определение 11.1. *Нека $k[x_1, \ldots, x_n]$ е пръстенът на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k. Полиномът $f \in k[x_1, \ldots, x_n]$ се нарича неразложим над k, ако f не е постоянен полином и всяко разлагане $f = gh$ в произведение на полиноми $g, h \in k[x_1, \ldots, x_n]$ има $g \equiv \mathrm{const}$ или $h \equiv \mathrm{const}$.*

Неразложимостта на полином зависи от полето, над което го разглеждаме. Например, $x^2 + 1 \in \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$ е неразложим над $\mathbb{Q}$ и $\mathbb{R}$, но се разлага в произведение на линейни множители $x^2 + 1 = (x + i)(x - i)$ над $\mathbb{C}$.

Твърдение 11.2. *Всеки неконстантен полином $f \in k[x_1, \ldots, x_n]$ с коефициенти от поле k се разлага в произведение $f = f_1 \ldots f_r$ на неразложими над k полиноми $f_i \in k[x_1, \ldots, x_n]$.*

Доказателство: Ще разсъждаваме с индукция по старшия моном $LM(f)$ на $f \in k[x_1, \ldots, x_n]$ относно произволна мономна наредба $>$. Преди всичко, полиномът $f \in k[x_1, \ldots, x_n]$ е непостоянен тогава и само тогава, когато $LM(f) > 1$. Нека x^α е минималният относно $>$ моном, който е различен от $1 \in k$. Тогава всеки полином $f \in k[x_1, \ldots, x_n]$ със старши моном $LM(f) = x^\alpha$ е неразложим над k, доколкото $f \not\equiv \mathrm{const}$ и за всяко разлагане $f = gh$ в произведение на полиноми $g, h \in k[x_1, \ldots, x_n]$, предположението $g \not\equiv \mathrm{const}$ води до

$$LM(f) = LM(g)LM(h) > 1.LM(h) = LM(h) \geq 1.$$

Оттук $LM(h) = 1$ и $h \equiv \mathrm{const}$. Това установява базата на индукцията.
Да допуснем, че всеки полином $g \in k[x_1, \ldots, x_n]$ със старши моном $LM(g) < LM(f)$ се разлага в произведение на неразложими над k полиноми на $x_1, \ldots, x_n$. Ако $f \in k[x_1, \ldots, x_n]$ е неразложим над k, то f е свое разлагане. Ако $f \in k[x_1, \ldots, x_n]$ е разложим над k, то съществуват неконстантни полиноми $g, h \in k[x_1, \ldots, x_n]$, така че $f = gh$. В резултат, $LM(g) > 1$ и $LM(h) > 1$, откъдето

$$LM(f) = LM(g)LM(h) > LM(h) > 1,$$

$$LM(f) = LM(g)LM(h) > LM(g) > 1.$$

Сега по индукционно предположение съществуват неразложими над k полиноми $f_1, \ldots, f_p, f_{p+1}, \ldots, f_r \in k[x_1, \ldots, x_n]$, така че $g = f_1 \ldots f_r$, $h = f_{p+1} \ldots f_r$ и $f = f_1 \ldots f_r$, Q.E.D.
За да установим единствеността на разлагането на полином $f \in k[x_1, \ldots, x_n]$ в произведение от неразложими над k множители е нужно да докажем, че ако неразложим полином дели произведение на други два полинома, то той дели поне един от множителите. Ще работим с индукция по броя на променливите. За целта да напомним някои свойства на пръстена $k[x_1]$ от полиноми на една променлива x_1 с коефициенти от поле k.

Лема 11.3. *За всеки идеал I в пръстена $k[x_1]$ от полиноми на една променлива x_1 с коефициенти от поле k съществува полином $f \in I$, който го поражда, $I = \langle f \rangle$.*

Ако f и $\widetilde{f}$ пораждат един и същи идеал $I = \langle f \rangle = \langle \widetilde{f} \rangle$, то съществува $a \in k^* = k \setminus \{0\}$, така че $\widetilde{f} = af$.

Доказателство: Ако $I = \{0\}$ е нулевият идеал, то $I = \langle 0 \rangle$ се поражда от тъждествено нулевия полином $0 \in k[x_1]$. За произволен ненулев идеал $I \triangleleft k[x_1]$ да разгледаме множеството

$$M := \{\deg f \,|\, 0 \not\equiv f \in I\}$$

от степените на ненулевите полиноми от I. В качеството си на множество от неотрицателни цели числа, M има минимален елемент $m \in M$. Твърдим, че произволен полином $f \in I$ от степен $\deg f = m$ поражда I. Наистина, от $f \in I \triangleleft k[x_1]$ следва, че $\langle f \rangle \subseteq I$. За обратното включване да отбележим, че при деление на произволен полином $g \in I$ с f получаваме представяне $g = fq + r$ чрез полиноми $q, r \in k[x_1]$, където $r \equiv 0$ или $\deg r < \deg f$. Доколкото $r = g - fq \in I$, допускането $r \not\equiv 0$ води до противоречие с минималността на $\deg f$. Следователно $r \equiv 0$ и $g = fq \in \langle f \rangle$. В резултат, $I \subseteq \langle f \rangle$, откъдето и $I = \langle f \rangle$.
Ако $\langle f \rangle = \langle \widetilde{f} \rangle$, то от $f \in \langle \widetilde{f} \rangle$ следва съществуването на $g \in k[x_1]$ с $f = \widetilde{f} g$. Аналогично, $\widetilde{f} \in \langle f \rangle$ води до наличие на $h \in k[x_1]$ с $\widetilde{f} = fh$. След заместване получаваме $f = fgh$ или $f(1 - gh) = 0 \in k[x_1]$. В областта на цялост $k[x_1]$ оттук следва $gh = 1$, доколкото $f \not\equiv 0 \in k[x_1]$. В резултат, $1 = LM(g)LM(h) \geq LM(g) \geq 1$ фиксира, че $LM(g) = LM(h) = 1$. С други думи, $g, h \in k^*$, Q.E.D.

Определение 11.4. *Да предположим, че поне един от полиномите $f_1, \ldots, f_s \in k[x_1]$ не е тъждествено нулев. Общият делител f на $f_1, \ldots, f_s$ се нарича техен най-голям общ делител и се бележи с $f = GCD(f_1, \ldots, f_s)$, ако f се дели на всеки общ делител h на $f_1, \ldots, f_s$.*

Ако f и $\widetilde{f}$ са най-големи общи делители на $f_1, \ldots, f_s \in k[x_1]$, то съществува $a \in k^*$, така че $\widetilde{f} = af$. Наистина, общият делител f на $f_1, \ldots, f_s$ дели най-големия общ делител $\widetilde{f}$, така че $\widetilde{f} = gf$ за подходящ полином $g \in k[x_1]$. Аналогично, общият делител $\widetilde{f}$ на $f_1, \ldots, f_s$ дели най-големия общ делител f, откъдето $f = h\widetilde{f}$ за $h \in k[x_1]$. В резултат, $f = ghf$ за ненулевия полином f в областта на цялост $k[x_1]$ води до $gh = 1$. Последното равенство на полиноми изисква $a := g = h^{-1} \in k^*$.

Лема 11.5. *Ако $f_1, \ldots, f_s$ са не едновременно нулеви полиноми на x_1 с коефициенти от поле k, то най-големият общ делител $GCD(f_1, \ldots, f_s)$ е пораждащ на идеала, определен от тях,*

$$\langle f_1, \ldots, f_s \rangle = \langle GCD(f_1, \ldots, f_s) \rangle.$$

Доказателство: Достатъчно е да проверим, че всеки пораждащ $f \in k[x_1]$ на идеала $\langle f_1, \ldots, f_s \rangle = \langle f \rangle$ изпълнява свойствата на най-голям общ делител $GCD(f_1, \ldots, f_s)$ на $f_1, \ldots, f_s$.
От една страна, $f_i \in \langle f_1, \ldots, f_s \rangle = \langle f \rangle$ води до $f_i = fg_i$ за подходящи полиноми $g_i \in k[x_1]$ и всички $1 \leq i \leq s$. По този начин, f се оказва общ делител на $f_1, \ldots, f_s$.
От друга страна, $f \in \langle f \rangle = \langle f_1, \ldots, f_s \rangle$ предоставя тъждеството на Безу

$$f = f_1 g_1 + \ldots + f_s g_s$$

за подходящи полиноми $g_1, \ldots, g_s \in k[x_1]$. Сега всеки общ делител h на $f_1, \ldots, f_s$ дели всички $f_i g_i$, а оттам и тяхната сума f. Това доказва, че $f = GCD(f_1, \ldots, f_s)$, Q.E.D.

Следствие 11.6. *Ако $f \in k[x_1]$ е неразложим над k полином на x_1, който дели произведението gh на полиномите $g, h \in k[x_1]$, то f дели g или f дели h.*

Доказателство: Нека $d = GCD(f, g)$ е най-голям общ делител на f и g. В качеството си на делител на неразложимия над k полином $f \in k[x_1]$, полиномът d е или от k^* или $f = ad$ се различава от d с мултипликативна константа $a \in k^*$. В случая $f = ad$ делимостта на g с d дава $g = dh$ за подходящ полином $h \in k[x_1]$, откъдето и $g = f(a^{-1}h)$ за $a^{-1}h \in k[x_1]$. Ако $d \in k^*$, то съгласно Лема 11.5 имаме

$$\langle f, g \rangle = \langle d \rangle = k[x_1].$$

Да разгледаме тъждеството на Безу

$$1 = fu + gv$$

за $1 \in k \subset k[x_1]$ с $u, v \in k[x_1]$. Умножавайки почленно с $h \in k[x_1]$ получаваме

$$h = fhu + ghv.$$

Двете събираеми от дясната страна се делят на f, така че тяхната сума h се дели на f, Q.E.D.
За да обобщим Следствие 11.6 за полиноми на произволен брой порменливи са нужни още две леми.

Лема 11.7. *Да предположим, че за произволни полиноми $v, w \in k[x_2, \ldots, x_n]$, делимостта на vw с неразложим над k полином $u \in k[x_2, \ldots, x_n]$ води до делимост на v с u или на w с u. Тогава за произволни полиноми $g, h \in k[x_1, x_2, \ldots, x_n]$, делимостта на gh с неразложим над k полином $u \in k[x_2, \ldots, x_n]$ води до делимост на g с u или на h с u.*

Доказателство: Да представим

$$g = \sum_{i=0}^{p} g_i x_1^i, \quad h = \sum_{i=0}^{q} h_i x_1^i$$

чрез $g_i, h_i \in k[x_2, \ldots, x_n]$ за някакви $p, q \in \mathbb{N} \cup \{0\}$. Тогава произведението

$$gh = \sum_{i=0}^{p+q} \left(\sum_{j=0}^{i} g_j h_{i-j} \right) x_1^i$$

се дели на $u \in k[x_2, \ldots, x_n]$ точно когато всеки полином

$$t_i := \sum_{j=0}^{i} g_j h_{i-j} \in k[x_2, \ldots, x_n]$$

се дели на u. Достатъчността на условието е ясна. Ако u дели gh в $k[x_1, x_2, \ldots, x_n]$, то съществува полином $f = \sum_{i=0}^{s} f_i x_1^i \in k[x_1, x_2, \ldots, x_n]$ с $f_i \in k[x_2, \ldots, x_n]$, така че

$$\sum_{i=0}^{s} (uf_i) x_1^i = uf = gh = \sum_{i=0}^{p+q} t_i x_1^i.$$

Определението за равенство на полиноми изисква $s = p+q$ и $uf_i = t_i$ за всички $0 \leq i \leq p+q$. С други думи, u дели t_i в $k[x_2, \ldots, x_n]$.
Да допуснем, че u дели gh, но не дели нито g, нито h. Това означава съществуване на индекси $0 \leq i \leq p$ и $0 \leq j \leq q$, така че u не дели g_i и не дели h_j. Да изберем минималните $0 \leq i_o \leq p$ и $0leqj_o \leq q$, така че u не дели g_{i_o} и h_{j_o}. Тогава делимостта на

$$t_{i_o+j_o} = (g_0 h_{i_o+j_o} + \ldots + g_{i_o-1} h_{j_o+1}) + g_{i_o} h_{j_o} + (g_{i_o+1} h_{j_o-1} + \ldots + g_{i_o+j_o} h_0)$$

с u и делимостта на $g_0, \ldots, g_{i_o-1}, h_0, \ldots, h_{j_o-1}$ с u води до делимост на $g_{i_o} h_{j_o}$ с u за $g_{i_o}, h_{j_o} \in k[x_2, \ldots, x_n]$. Съгласно предположението, u трябва да дели g_{i_o} или h_{j_o}. Полученото противоречие показва, че u дели g или h, Q.E.D.

Лема 11.8. *Да предположим, че за произволни $v, w \in k[x_2, \ldots, x_n]$ делимостта на vw с неразложим над k полином $u \in k[x_2, \ldots, x_n]$ води до делимост на v или на w с u. Тогава всеки неразложим над k полином $f \in k[x_1, x_2, \ldots, x_n]$, който е от положителна степен относно x_1, е полином $f \in k(x_2, \ldots, x_n)[x_1]$ на x_1, който е неразложим над полето $k(x_2, \ldots, x_n)$ на рационалните функции на $x_2, \ldots, x_n$.*

Доказателство: По определение, трябва да докажем, че ако $f = gh$ за $g, h \in k(x_2, \ldots, x_n)[x_1]$, то $g \in k(x_2, \ldots, x_n)$ или $h \in k(x_2, \ldots, x_n)$. За целта да представим

$$g = \sum_{i=0}^{p} g_i x_1^i, \quad h = \sum_{i=0}^{q} h_i x_1^i$$

чрез $g_i, h_j \in k(x_2, \ldots, x_n)$ за $0 \leq i \leq p$, $0 \leq j \leq q$, $p, q \in \mathbb{N} \cup \{0\}$. Да означим с $d \in k[x_2, \ldots, x_n]$ произведението на знаменателите на $g_0, \ldots, g_p, h_0, \ldots, h_q$. Тогава

$$d^2 f = (dg)(dh) \in k[x_1, x_2, \ldots, x_n]$$

с $dg, dh \in k[x_1, x_2, \ldots, x_n]$. Разлагаме $d = d_1 \ldots d_m$ в произведение на неразложими над k полиноми $d_i \in k[x_2, \ldots, x_n]$. Съгласно Лема 11.7, всяко d_i дели dg или dh в $k[x_1, x_2, \ldots, x_n]$. След съкращаване на $d^2 = d_1^2 \ldots d_m^2 \in k[x_2, \ldots, x_n]$ от двете страни получаваме

$$f = \widetilde{g}\widetilde{h}$$

за подходящи полиноми $\widetilde{g}, \widetilde{h} \in k[x_1, x_2, \ldots, x_n]$. Сега неразложимостта на $f \in k[x_1, x_2, \ldots, x_n]$ над k води до $\widetilde{g} \in k$ или $\widetilde{h} \in k$. Следователно $dg \in k[x_2, \ldots, x_n]$ или $dh \in k[x_2, \ldots, x_n]$, така че $g \in k(x_2, \ldots, x_n)$ или $h \in k(x_2, \ldots, x_n)$, Q.E.D.
С това сме готови да докажем следната

Теорема 7. *Ако неразложимият над k полином $f \in k[x_1, \ldots, x_n]$ дели произведението gh на полиноми $g, h \in k[x_1, \ldots, x_n]$, то f дели g или f дели h.*

Доказателство: Ще разсъждаваме с индукция по броя на променливите n. За Следствие 11.6 решава въпроса.
Да допуснем, че сме доказали теоремата за полиноми на $n-1$ променливи. Съгласно Лема 11.7, без ограничение ще считаме, че $f \in k[x_1, \ldots, x_n]$ зависи от x_1, т.е. $f = \sum_{i=0}^{s} f_i x_1^i$ с $f_i \in k[x_2, \ldots, x_n]$ и $f_s \not\equiv 0$ за подходящо естествено s. Прилагайки Лема 11.8 към f получаваме, че полиномът $f \in k(x_2, \ldots, x_n)[x_1]$ на x_1 е неразложим над полето $k(x_2, \ldots, x_n)$ на рационалните функции на $x_2, \ldots, x_n$ с коефициенти от k. Разглеждаме $g, h \in k(x_2, \ldots, x_n)[x_1]$ като полиноми на x_1 с коефициенти от $k(x_2, \ldots, x_n)$. Прилагаме Следствие **??** и получаваме делимост на g и h с f в $k(x_2, \ldots, x_n)[x_1]$. След евентуална размяна между g и h това означава съществуване на полином $t = \sum_{i=0}^{r} t_i x_1^i \in k(x_2, \ldots, x_n)[x_1]$ на x_1 с коефициенти $t_i \in k(x_2, \ldots, x_n)$, така че

$$g = ft = \left(\sum_{i=0}^{s} f_i x_1^i\right)\left(\sum_{i=0}^{r} t_i x_1^i\right).$$

Да означим с $d \in k[x_2, \ldots, x_n]$ произведението на знаменателите на $t_0, \ldots, t_r$. Тогава

$$dg = f(dt) \in k[x_1, x_2, \ldots, x_n]$$

с $dt \in k[x_1, x_2, \ldots, x_n]$. Разлагаме $d = d_1 \ldots d_m$ в произведение от неразложими над k полиноми $d_i \in k[x_2, \ldots, x_n]$. Съгласно Лема 11.7, всяко d_i дели $f \in k[x_1, x_2, \ldots, x_n]$ или $dt \in k[x_1, x_2, \ldots, x_n]$, доколкото дели тяхното произведение. Неразложимите над k полиноми $d_i \in k[x_2, \ldots, x_n]$ са непостоянни по определение. Следователно, ако d_i дели f, то съществува $a \in k^*$, така че $f = d_i a$, благодарение на неразложимостта на f над k. Но тогава $f = d_i a \in k[x_2, \ldots, x_n]$

не зависи от x_1, противно на предположението. По този начин установихме, че всички d_i делят dt и след съкращаване на $d = d_1 \dots d_m$ получаваме

$$g = f\widetilde{t}$$

за някакъв полином $\widetilde{t} \in k[x_1, x_2, \dots, x_n]$. С други думи, f дели g в $k[x_1, x_2, \dots, x_n]$, Q.E.D.

Преди да изведем от Теорема 7 единствеността на разлагането на $f \in k[x_1, \dots, x_n]$ в произведение от неразложими над k полиноми $f_i \in k[x_1, \dots, x_n]$, ще докажем следното

Следствие 11.9. *Нека $f = \sum_{i=0}^{p} f_i x_1^i$ и $g = \sum_{i=0}^{q} g_i x_1^i$ с $f_i, g_i \in k[x_2, \dots, x_n]$ са полиноми на $x_1, \dots, x_n$ с $p > 0$, $f_p \not\equiv 0$ и $q > 0$, $g_q \not\equiv 0$. В такъв случай, f и g имат общ множител $h = \sum_{i=0}^{r} h_i x_1^i \in k[x_1, x_2, \dots, x_n]$ с $h_i \in k[x_2, \dots, x_n]$ и $r > 0$, тогава и само тогава, когато f и g имат общ множител в пръстена $k(x_2, \dots, x_n)[x_1]$, който зависи от x_1.*

Доказателство: Ясно е, че ако $h = \sum_{i=0}^{r} h_i x_1^i$ с $h_i \in k[x_2, \dots, x_n]$ е общ множител на f и g от $k[x_1, x_2, \dots, x_n]$, то $h \in k[x_2, \dots, x_n]$ е и общ множител на f и g от $k[x_2, \dots, x_n][x_1]$, зависещ от x_1.
Нека $f, g \in k[x_1, x_2, \dots, x_n]$ имат общ множител $\widetilde{h} \in k(x_2, \dots, x_n)[x_1]$, зависещ от x_1. Тогава

$$f = \widetilde{f}\widetilde{h} \quad \text{за} \quad \widetilde{f} \in k(x_2, \dots, x_n)[x_1] \quad \text{и}$$

$$g = \widetilde{g}\widetilde{h} \quad \text{за} \quad \widetilde{g} \in k(x_2, \dots, x_n)[x_1].$$

Ако $\widetilde{h} = \sum_i \widetilde{h}_i x_1^i$, $\widetilde{f} = \sum_i \widetilde{f}_i x_1^i$, $\widetilde{g} = \sum_i \widetilde{g}_i x_1^i$ с $\widetilde{h}_i, \widetilde{f}_i, \widetilde{g}_i \in k(x_2, \dots, x_n)$ и $\widetilde{h_r} \not\equiv 0$ за някое $r > 0$, то да означим с $d \in k[x_2, \dots, x_n]$ произведението на знаменателите на всички $\widetilde{h}_i, \widetilde{f}_i, \widetilde{g}_i$. Тогава $h := d\widetilde{h}$, $f_1 := d\widetilde{f}$ и $g_1 := d\widetilde{g}$ са полиноми от $k[x_1, x_2, \dots, x_n]$, изпълняващи равенствата

$$d^2 f = h f_1 \quad \text{и} \quad d^2 g = h g_1.$$

Полиномът $h \in k[x_1, x_2, \dots, x_n]$ от положителна степен относно x_1 има неразложим над k делител $h' \in k[x_1, x_2, \dots, x_n]$, който е от положителна степен относно x_1. Съгласно Теорема 7, полиномът h' дели $d^2 \in k[x_2, \dots, x_n]$ или h' доколкото дели тяхното произведение $d^2 f$. Понеже $d^2 \in k[x_2, \dots, x_n]$ е от нулева степен относно x_1, полиномът $h' \in k[x_1, x_2, \dots, x_n]$ с положителна степен относно x_1 дели полинома $f \in k[x_1, x_2, \dots, x_n]$. Аналогично, h' дели g, така че $h' \in k[x_1, x_2, \dots, x_n]$ се оказва общ множител на f и g в $k[x_1, x_2, \dots, x_n]$, който е с положителна степен относно x_1, Q.E.D.

Теорема 8. *Ако $f = f_1 \dots f_r$ и $f = g_1 \dots g_s$ са две разлагания на неконстантен полином $f \in k[x_1, \dots, x_n]$ в произведение от неразложими над k множители $f_i, g_j \in k[x_1, \dots, x_n]$, то $r = s$ и съществуват пермутация $\sigma \in S_r$ и ненулеви мултипликативни константи $a_i \in k^*$, така че*

$$g_{\sigma(i)} = a_i f_i \quad \textit{за} \quad \forall 1 \leq i \leq r.$$

Доказателство: Без ограничение на общността можем да считаме, че броят на множителите r в първото разлагане не надминава броя на множителите s във второто разлагане, $r \leq s$. Ще работим с индукция по $r \in \mathbb{N}$. Ако $f_1 = g_1 \dots g_s$, то неразложимият над k полином f_1 дели $g_1 \dots g_s$ и съгласно Теорема 7, f_1 дели някое g_j, $1 \leq j \leq s$. Неразложимостта на f_1 и g_j гарантира съществуването на $a_1 \in k^*$, така че $g_j = a_1 f_1$. В областта на цялост $k[x_1, \dots, x_n]$ разделяме почленно равенството $f_1 = g_1 \dots g_{j-1} a_1 f_1 g_{j+1} \dots g_s$ с $f_1 \not\equiv 0$ и получаваме $1 =$

$g_1 \dots g_{j-1} a_1 g_{j+1} \dots g_s$. Ако допуснем, че $s > 1$, то относно произволна мономна наредба $>$ в $k[x_1, \dots, x_n]$, старшите мономи $LM(g_k) > 1$, откъдето

$$1 = LM(1) = \prod_{k \neq j} LM(g_k) > 1.$$

Противоречието доказва, че $s = 1$ и установява твърдението на теоремата за $r = 1$.

Да допуснем, че сме доказали теоремата за произволни двойки разлагания в които поне едното е с по-малко от r неразложими над k множителя. Тогава от

$$f_1 \dots f_r = g_1 \dots g_s$$

следва, че f_r дели $g_1 \dots g_s$. Съгласно Теорема 7, съществува $1 \leq j \leq s$, така че f_r дели g_j. Неразложимостта на f_r и g_j изисква $g_j = a_r f_r$ за подходяща мултипликативна константа $a_r \in k^*$. Съкращавайки равенството

$$f_1 \dots f_{r-1} f_r = g_1 \dots g_{j-1} a_r f_r g_{j+1} \dots g_s$$

с $f_r \not\equiv 0$ в областта $k[x_1, \dots, x_n]$, получаваме

$$f_1 \dots f_{r-1} = g_1 \dots g_{j-1} (a_r g_{j+1}) \dots g_s.$$

От индукционното предположение следва, че $r - 1 = s - 1$ и съществуват взаимно-еднозначно изображение

$$\sigma' : \{1, \dots, r-1\} \longrightarrow \{1, \dots, j-1, j+1, \dots, r\},$$

както и $a_i \in k^*$, така че $g_{\sigma'(i)} = a_i f_i$ за всички $1 \leq i \leq r-1$. Остава само да отбележим, че изображението

$$\sigma : \{1, \dots, r\} \longrightarrow \{1, \dots, r\} \quad \text{с}$$
$$\sigma(i) := \sigma'(i) \quad \text{за} \quad \forall 1 \leq i \leq r-1 \quad \text{и}$$
$$\sigma(r) := j$$

е пермутация на $1, \dots, r$, Q.E.D.

Задачи

Задача 11.10. *Нека $g_1, \dots, g_t \in \mathbb{R}[x]$ са неразложими над $\mathbb{R}$ полиноми на x и $d_1, \dots, d_t$ са произволни естествени числа Да се докаже, че най-големият общ делител $GCD(g, g')$ на полинома $g = g_1^{d_1} \dots g_t^{d_t}$ и неговата производна g' е равен на*

$$GCD(g, g') = g_1^{d_1 - 1} \dots g_t^{d_t - 1}$$

с точност до ненулева реална мултипликативна константа.

Упътване: Първо докажете, че

$$GCD(g_1 \dots g_t, \sum_{i=1}^{t} d_i g_1 \dots g_{i-1} g_i' g_{i+1} \dots g_t) = 1$$

и оттук изведете, че $g_1^{d_1 - 1} \dots g_t^{d_t - 1}$ поражда идеала $\langle g, g' \rangle \triangleleft k[x]$.