Manuel Kauers
RISC-Linz

Hagenberg, January 13, 2003

Computer Algebra Exercises
Solution 7

Ex. (31) Let

$$\begin{aligned} a(x,y) &= xy^2 - x^3y - 2x^2y + xy + 2x^4 - 2x^2 \\ &= xy^2 + (-x^3 - 2x^2 + x)y + (2x^4 - 2x^2) \\ b(x,y) &= 2x^2y^2 - 4x^3y + 4x^3. \end{aligned}$$

We are about to compute the resultant of a and b with respect to y. Writing

$$m = n = \deg_y(a) = \deg_y(b) = 2.$$

and

$$d = \max_{0\le i\le m} ||a_i|| = 4, \qquad e = \max_{0\le i\le n} ||b_i|| = 4,$$

we get the coefficient bound

$$B = 2(m+n)!d^n e^m = 2\cdot 4!\cdot 4^2\cdot 4^2 = 12\,288.$$

We compute the resultant by the algorithm RES_MOD. The following table shows the intermediate results.

P	p	c_p	c
1	2	FAIL	0
1	3	FAIL	0
1	5	FAIL	0
1	7	FAIL	0
1	11	FAIL	0
1	17	FAIL	0
1	19	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$	$8x^{12} + 3x^{11} - 3x^9 + 8x^8$
19	23	$8x^{12} + 7x^{11} + 16x^9 + 8x^8$	$8x^{12} - 16x^{11} + 16x^9 + 8x^8$
437	29	$8x^{12} + 13x^{11} + 16x^9 + 8x^8$	$8x^{12} - 16x^{11} + 16x^9 + 8x^8$
12 673	Stop: $P = 12\,673 > 12\,288 = B$		

We get the result

$$\mathrm{Res}_y(a,b) = 8x^{12} - 16x^{11} + 16x^9 + 8x^8.$$

For the computation of the c_p, we show the intermediate results for $p = 19$ only.[1] For failing primes, the computation is not interesting, the failure is just due to the fact that there are to few evaluation points. For the other contributing primes, the table of intermediate results looks similar.

For the shown $p = 19$, the degree bound amounts to $B = 17$.

[1]The author wishes to thank Tobias Beck for finding a subtle bug in the code which generated the data in the table on the following page.

β	$a_p(\beta, y)$	$b_p(\beta, y)$	c_β	c_p
0	0	0	FAIL	0
1	$y^2 + 17y$	$2y^2 + 15y + 4$	16	16
2	$2y^2 + 5y + 5$	$8y^2 + 6y + 7$	18	$2x + 14$
3	$3y^2 + 15y + 11$	$18y^2 + 6y + 1$	17	$8x^2 + 16x + 11$
4	$4y^2 + 3y + 5$	$13y^2 + 10y + 17$	8	$15x^3 + 13x^2 + 10x + 15$
5	$5y^2 + y + 3$	$12y^2 + 13y + 11$	2	$7x^4 + 2x^3 + 11x^2 + 2x + 13$
6	$6y^2 + 3y + 12$	$15y^2 + 10y + 16$	4	$9x^5 + 5x^4 + 7x^3 + 17x + 16$
7	$7y^2 + 3y + 11$	$3y^2 + 15y + 9$	12	$18x^6 + 11x^5 + x^4 + x^3 + 10x^2 + 14x + 18$
8	$8y^2 + 14y + 8$	$14y^2 + 4y + 6$	8	$17x^7 + 17x^6 + 13x^5 + 7x^4 + 10x^3 + 16x^2 + 3x + 9$
9	$9y^2 + 11y + 2$	$10y^2 + 10y + 5$	14	$13x^8 + 5x^7 + 9x^6 + 2x^5 + 4x^4 + 2x^3 + 10x^2 + 12x + 16$
10	$10y^2 + 7y + 2$	$10y^2 + 9y + 5$	9	$18x^9 + x^8 + 9x^7 + 16x^6 + 18x^5 + 4x^4 + 13x^3 + 11x^2 + 6x + 15$
11	$11y^2 + 15y + 8$	$14y^2 + 15y + 6$	6	$18x^9 + x^8 + 9x^7 + 16x^6 + 18x^5 + 4x^4 + 13x^3 + 11x^2 + 6x + 15$
12	$12y^2 + 10y + 11$	$3y^2 + 4y + 9$	9	$18x^9 + x^8 + 9x^7 + 16x^6 + 18x^5 + 4x^4 + 13x^3 + 11x^2 + 6x + 15$
13	$13y^2 + 5y + 12$	$15y^2 + 9y + 16$	3	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$
14	$14y^2 + 13y + 3$	$12y^2 + 6y + 11$	10	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$
15	$15y^2 + 9y + 5$	$13y^2 + 9y + 17$	13	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$
16	$16y^2 + 6y + 11$	$18y^2 + 13y + 1$	8	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$
17	$17x^2 + 17y + 5$	$8y^2 + 13y + 7$	17	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$
18	$18y^2 + 17y$	$2y^2 + 4y + 4$	16	$8x^{12} + 3x^{11} + 16x^9 + 8x^8$

Ex. (32) Let

$$\begin{aligned} f_1(x,y,z) &= 2xy - yz + 2z \\ f_2(x,y,z) &= x^2 + yz - 1 \\ f_3(x,y,z) &= xz + yz - 2x. \end{aligned}$$

Then, by Maple,

$$\begin{aligned} r_{zy}(x) &= \mathrm{Res}_z(\mathrm{Res}_y(f_1,f_2), \mathrm{Res}_y(f_1,f_3)) \\ &= -8x^7 + 32x^6 + 64x^5 + 16x^4 - 56x^3 + 16x^2, \\ r_{zx}(y) &= \mathrm{Res}_z(\mathrm{Res}_x(f_1,f_2), \mathrm{Res}_x(f_1,f_3)) \\ &= 16y^8 - 128y^6 + 320y^5 - 576y^4 + 512y^3 - 256y^2, \\ r_{yx}(z) &= \mathrm{Res}_y(\mathrm{Res}_x(f_1,f_2), \mathrm{Res}_x(f_1,f_3)) \\ &= -64z^8 + 672z^7 - 1\,792z^6 + 2\,304z^5 - 1\,024z^4 + 512z^3. \end{aligned}$$

Now, by Winker, each root of the first system is also a root of the latter. We can therefore go through all roots of the latter system and check if they satisfy the first.

But what are the roots of the latter system? First, we can factor r_{zy} by Maple and find

$$r_{zy}(x) = -8x^2(x^5 - 8x^3 - 4x^4 + 7x - 2x^2 - 2).$$

This has the roots $x = 0$ and $x = \alpha$ where α is an algebraic extension such that

$$\mathbb{Q}(\alpha) = \mathbb{Q}[x] / \langle x^5 - 8x^3 - 4x^4 + 7x - 2x^2 - 2 \rangle.$$

Now, we can factor the second polynomial in $\mathbb{Q}(\alpha)$. This yields

$$r_{zx}(y) = 4(y-2)y^2(2y + (-2\alpha^4 + 7\alpha^3 + 20\alpha^2 + 13\alpha - 10))u_1(y)$$

where $u_1 \in \mathbb{Q}(\alpha)[y]$ is an ugly irreducible factor. Hence, r_{zx} has the roots $y = 0$, $y = 2$,

$$y = \alpha^4 - \tfrac{7}{2}\alpha^3 - 10\alpha^2 - \tfrac{13}{2}\alpha + 5,$$

and $y = \beta$, where β is a new algebraic extension of $\mathbb{Q}(\alpha)$ such that

$$\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)[y] / \langle u_1(y) \rangle.$$

Finally, for the factorization of r_{yx} over $\mathbb{Q}(\alpha,\beta)$ brings

$$r_{yx}(z) = \tfrac{1}{8}z^3 \cdot (2z + \alpha^4 - 4\alpha^3 - 8\alpha^2 - 4\alpha + 3) \cdot u_2(z)$$

where $u_2(z) \in \mathbb{Q}(\alpha,\beta)$ is again an irreducible factor. Let γ be an algebraic number which vanishes on $u_2(y)$, i.e. let γ be such that

$$\mathbb{Q}(\alpha,\beta,\gamma) = \mathbb{Q}(\alpha,\beta)[z] / \langle u_2(z) \rangle.$$

By some intuition (called Maple), we know that the solutions of the system can be expressed in $\mathbb{Q}(\alpha)$, and we allow ourselves to ignore root candidates that involve β or γ.

The set of solution candidates hence amounts to

$$\{0,\alpha\}\times\{0,2,\alpha^4-\tfrac{7}{2}\alpha^3-10\alpha^2-\tfrac{13}{2}\alpha+5\}\times\{0,-\tfrac{1}{2}\alpha^4+2\alpha^3+4\alpha^2+2\alpha-\tfrac{3}{2}\}.$$

We have to check all of them now.

First, if $x=0$, then

$$\begin{aligned} f_1(0,y,z) &= -yz\\ f_2(0,y,z) &= yz-1\\ f_3(0,y,z) &= yz. \end{aligned}$$

The third equation requires $yz=0$ in contradiction to the second equation which requires $yz=1$. Hence, $x\neq 0$ and it only remains $x=\alpha$.

For $y=0$, we get

$$\begin{aligned} f_1(\alpha,0,z) &= 2z\\ f_2(\alpha,0,z) &= \alpha^2-1\\ f_3(\alpha,0,z) &= \alpha z-2\alpha. \end{aligned}$$

The first equation requires $z=0$, and with this the third equation would imply $\alpha=0$ which is impossible. Hence, $y\neq 0$. For $y=2$, we get

$$\begin{aligned} f_1(\alpha,2,z) &= 4\alpha\\ f_2(\alpha,2,z) &= \alpha^2+2z-1\\ f_3(\alpha,2,z) &= \alpha z+2z-2\alpha. \end{aligned}$$

This time, the first equation would imply $\alpha=0$ which still cannot be. It remains the possibility

$$y=y_0:=\alpha^4-\tfrac{7}{2}\alpha^3-10\alpha^2-\tfrac{13}{2}\alpha+5.$$

We now turn to z. First, for $z=0$, we receive

$$\begin{aligned} f_1(\alpha,y_0,z) &= 2\alpha y_0\\ f_2(\alpha,y_0,z) &= \alpha^2-1\\ f_3(\alpha,y_0,z) &= -2\alpha \end{aligned}$$

The first and the last equation lead to contradicitions. It only remains the possibility

$$z=z_0:=-\tfrac{1}{2}\alpha^4+2\alpha^3+4\alpha^2+2\alpha-\tfrac{3}{2}.$$

Finally, we get

$$\begin{aligned} &f_1(x_0,y_0,z_0)=2x_0y_0-y_0z_0+2z_0\\ =\ &\tfrac{1}{8}\alpha^8-\tfrac{15}{4}\alpha^7-2\alpha^6+\tfrac{123}{4}\alpha^5+56\alpha^4+\tfrac{59}{4}\alpha^3-27\alpha^2-\tfrac{23}{4}+\tfrac{9}{2}=0,\\ &f_2(x_0,y_0,z_0)=x_0^2+y_0z_0-1\\ =\ &-\tfrac{1}{2}\alpha^8+\tfrac{15}{4}\alpha^7+2\alpha^6-\tfrac{115}{4}\alpha^5-64\alpha^4-\tfrac{123}{4}\alpha^3+23\alpha^2+\tfrac{79}{4}\alpha-\tfrac{17}{2}=0,\\ &f_3(x_0,y_0,z_0)=x_0z_0+y_0z_0-2x_0\\ =\ &-\tfrac{1}{2}\alpha^8+\tfrac{15}{4}\alpha^7+2\alpha^6-\tfrac{117}{4}\alpha^5-62\alpha^4-\tfrac{107}{4}\alpha^3+24\alpha^2+\tfrac{65}{4}\alpha-\tfrac{15}{2}=0, \end{aligned}$$

which proves that (x_0, y_0, z_0) actually describes the solution set of the system under consideration.

By Maple, we can verify that there are no other solutions of the system, and using numerics it can be found that α actually corresponds to five complex values, i.e. the the system has five solutions.

Ex. (33) We consider the system given by the polynomials

$$\begin{aligned} f_1(x,y,z) &= xz - xy^2 - 4x^2 - \tfrac{1}{4} \\ f_2(x,y,z) &= y^2 z + 2x + \tfrac{1}{2} \\ f_3(x,y,z) &= x^2 z + y^2 + \tfrac{1}{2}x. \end{aligned}$$

Any value of z which is part of a solution of the system, must be a root of both

$$r_{xy}(z) = \Big(- \tfrac{5}{64}z^5 - \tfrac{1}{8}z^4 - \tfrac{3}{64}z^3 + \tfrac{13}{32}z^2 + \tfrac{51}{32}z - \tfrac{15}{16}\Big)^4$$

and

$$\begin{aligned} r_{yx}(z) = \Big(&- 10z^{11} - \tfrac{89}{4}z^{10} - \tfrac{163}{8}z^9 + \tfrac{385}{16}z^8 + \tfrac{9679}{32}z^7 + \tfrac{1201}{4}z^6 + \\ &\tfrac{11641}{32}z^5 - \tfrac{1005}{8}z^4 - \tfrac{45195}{16}z^3 - \tfrac{5715}{4}z^2 + \tfrac{6075}{4}z\Big)^2 \end{aligned}$$

and hence of its greatest common divisor

$$\gcd(r_{xy}, r_{yx}) = \tfrac{1}{25}(-5z^5 - 8z^4 - 3z^3 + 26z^2 + 102z - 60)^2;$$

This representation is already a factorisation, so let α be an algebraic number such that

$$\mathbb{Q}(\alpha) = {}^{\mathbb{Q}[z]}\!\big/_{\langle -5z^5 - 8z^4 - 3z^3 + 26z^2 + 102z - 60\rangle}.$$

We know that any solution (x, y, z) to the system will have $z = \alpha$.

Now consider the variable x. The resultant hacking leads to

$$\begin{aligned} r_{zy}(x) &= \Big(- \tfrac{5}{16}x^3 - 2x^4 + \tfrac{21}{8}x^5 - 4x^6 + \tfrac{27}{2}x^7 - 2x^8\Big)^4 \\ r_{yz}(x) &= \tfrac{1}{4096}x^4(-864x^5 + 128x^6 - 168x^3 + 256x^4 + 20x + 128x^2)^2 \\ \gcd(r_{zy}, r_{yz}) &= u_1(x) \cdot (x - \tfrac{8323}{1388} - \tfrac{457}{347}\alpha + \tfrac{1219}{2776}\alpha^2 + \tfrac{769}{1388}\alpha^3 + \tfrac{705}{2776}\alpha^4)^2 x^6 \end{aligned}$$

where $u_1(x) \in \mathbb{Q}(\alpha)[x]$ is an ugly irreducible polynomial of degree 4. We denote by β an algebraic number which is root of this polynomial, i.e.

$$\mathbb{Q}(\alpha, \beta) = {}^{\mathbb{Q}(\alpha)[x]}\!\big/_{\langle u_1(x)\rangle}.$$

As possible values for x, we now have the candidates $x = 0$, $x = \beta$, and

$$x = \tfrac{8323}{1388} + \tfrac{457}{347}\alpha - \tfrac{1219}{2776}\alpha^2 - \tfrac{769}{1388}\alpha^3 - \tfrac{705}{2776}\alpha^4.$$

Finally, consider the candidates for the coordinate y. We have

$$\begin{aligned} r_{xz}(y) &= \tfrac{1}{4}y^2(2y^{12} + 54y^{10} + \tfrac{335}{4}y^8 + \tfrac{169}{4}y^7 + \tfrac{109}{16}y^4 - \tfrac{5}{4}y^2) \\ r_{zx}(y) &= -432y^{22} - 11680y^{20} - 18516y^{18} - \tfrac{19317}{2}y^{16} - \tfrac{4431}{2}y^{14} \\ &\quad - \tfrac{9119}{16}y^{12} - \tfrac{10757}{32}y^{10} - \tfrac{2515}{64}y^8 + \tfrac{1109}{128}y^6 - \tfrac{97}{16}y^4 + \tfrac{5}{8}y^2 \\ \gcd(r_{xz}, r_{zx}) &= y^2(y^2 + \tfrac{16567}{694} + \tfrac{6295}{1388}\alpha - \tfrac{2405}{1388}\alpha^2 - \tfrac{3017}{1388}\alpha^3 - \tfrac{1445}{1388}\alpha^4)u_2(y) \end{aligned}$$

where $u_2(y)$ is again an ugly irreducible factor which we don't want to get to close to. For the candidates of y, we get $y = 0$, $y = \gamma_1$ and $y = \gamma_2$ where γ_1, γ_2 are new algebraic numbers defined by

$$\mathbb{Q}(\alpha, \beta, \gamma_1) = {}^{\mathbb{Q}(\alpha,\beta)[y]}\Big/_{\langle y^2 + \frac{16567}{694} + \frac{6295}{1388}\alpha - \frac{2405}{1388}\alpha^2 - \frac{3017}{1388}\alpha^3 - \frac{1445}{1388}\alpha^4\rangle}$$
$$\mathbb{Q}(\alpha, \beta, \gamma_1, \gamma_2) = {}^{\mathbb{Q}(\alpha,\beta,\gamma_1)[y]}\Big/_{\langle u_2(y)\rangle}.$$

Again, by some strange intuition, we know that β and γ_2 don't appear in the final solution of the original system, so the candidate set is

$$\{0, \tfrac{8323}{1388} + \tfrac{457}{347}\alpha - \tfrac{1219}{2776}\alpha^2 - \tfrac{769}{1388}\alpha^3 - \tfrac{705}{2776}\alpha^4\} \times \{0, \gamma_1\} \times \{\alpha\}.$$

Plugging $x = 0$ into the system, we get

$$\begin{aligned} f_1(0, y, z) &= -\tfrac{1}{4} \\ f_2(0, y, z) &= y^2 z + \tfrac{1}{2} \\ f_3(0, y, z) &= y^2, \end{aligned}$$

i.e. the first equation cannot be satisfied. It only remains the possibility

$$x = x_0 := \tfrac{8323}{1388} + \tfrac{457}{347}\alpha - \tfrac{1219}{2776}\alpha^2 - \tfrac{769}{1388}\alpha^3 - \tfrac{705}{2776}\alpha^4.$$

Plugging $y = 0$ into the system leads to

$$\begin{aligned} f_1(x, 0, z) &= xz - 4x^2 - \tfrac{1}{4} \\ f_2(x, 0, z) &= 2x + \tfrac{1}{2} \\ f_3(x, 0, z) &= x^2 z + \tfrac{1}{2}x. \end{aligned}$$

The constraint f_2 would require $x = -\frac{1}{4}$ which is inconsistent with what we know so far about x. It only remains $y = \gamma_1$.

Finally, plugging $(x, y, z) = (x_0, \gamma_1, \alpha)$ into the system leads to

$$\begin{aligned} f_1(x_0, \gamma_1, \alpha) &= x_0\alpha - \alpha\gamma_1^2 - 4x_0^2 - \tfrac{1}{4} = 0 \\ f_2(x_0, \gamma_1, \alpha) &= \gamma_1^2\alpha + 2x_0 + \tfrac{1}{2} = 0 \\ f_3(x_0, \gamma_1, \alpha) &= x_0^2\alpha + \gamma_1^2 + \tfrac{1}{2}x_0 = 0, \end{aligned}$$

i.e. this is really a solution.

Ex. (34) [taken from Winkler, page 242f]

By t denote the degree of a, and write $a = a_t + \cdots + a_0$ where a_i is a homogenous polynomial of degree i. Choose elements $c_1, \ldots, c_r \in K$ with the property that $c_r \neq 0$ and $a_t(c_1, \ldots, c_r) \neq 0$. Such c_i exist if K is sufficiently large. Let

$$\begin{aligned} \hat{a}(x_1, \ldots, x_r) &= a(x_1 + x_1 c_r, \ldots, x_{r-1} + c_{r-1}x_r, c_r x_r) \\ \hat{b}(x_1, \ldots, x_r) &= b(x_1 + x_1 c_r, \ldots, x_{r-1} + c_{r-1}x_r, c_r x_r). \end{aligned}$$

We claim that $(\alpha_1, \ldots, \alpha_r) \in K^r$ is a common root of $\hat{a}$ and $\hat{b}$ if and only if $(\alpha_1 + c_1\alpha_r, \ldots, \alpha_{r-1} + c_{r-1}\alpha_r, c_r\alpha_r)$ is a common root of a and b.

For the direction from the left to the right, assume that $(\alpha_1, \dots, \alpha_r)$ is a common root of $\hat{a}$ and $\hat{b}$. We have to show that $(\alpha_1 + c_1\alpha_r, \dots, \alpha_{r-1} + c_{r-1}\alpha_r, c_r\alpha_r)$ is a root of both a and b. This is immediate by the construction of $\hat{a}$ and $\hat{b}$:

$$\begin{aligned} 0 &= \hat{a}(\alpha_1, \alpha_2, \dots, \alpha_r) \\ &= a(\alpha_1 + \alpha_1 c_r, \dots, \alpha_{r-1} + c_{r-1}\alpha_r, c_r\alpha_r), \\ 0 &= \hat{b}(\alpha_1, \alpha_2, \dots, \alpha_r) \\ &= b(\alpha_1 + \alpha_1 c_r, \dots, \alpha_{r-1} + c_{r-1}\alpha_r, c_r\alpha_r) \end{aligned}$$

Ex. (35) [taken from Bosch, Corollary 9 on page 173]

First, it is immediate from the form of the Sylvester matrix that

$$\operatorname{Res}(\alpha f, \beta g) = \alpha^{\deg g}\beta^{\deg f}\operatorname{Res}(f, g)$$

by usual determinant manipulation rules. Using this, we can assume without loss of generality that f and g be monic.

Now, assume that $f(x) = x - \alpha$ and $g(x) = g_m x^m + \dots + g_0$. Then

$$\operatorname{Res}(f, g) = \det \begin{pmatrix} 1 & 0 & \dots & 0 & g_m \\ -\alpha & 1 & \ddots & \vdots & g_{m-1} \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots \\ 0 & \dots & 0 & -\alpha & g_0 \end{pmatrix} = g(\alpha).$$

As for the general case, we conclude from the determinant multiplicity that

$$\operatorname{Res}(ab, c) = \operatorname{Res}(a, c) \cdot \operatorname{Res}(b, c).$$

Hence, a successive decomposition of f leads to

$$\operatorname{Res}(f, g) = \prod_{i=1}^{n} g(\alpha_i).$$

Expanding the definition of g, we get the desired form

$$\operatorname{Res}(f, g) = \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$