WOLFGANG K. SEILER
Tel. 2515

B6,26, A4.18

10. Juni 2020

Modulklausur Computeralgebra

Aufgabe 1: (*10 Punkte*)
Wir betrachten die Polynome $f = 2X^4 + 6X^3 - 30X^2 + 32X - 24$ und $g = 2X^4 - 4X^2 - 6X - 4$ aus $\mathbb{Z}[X]$.

a) Bestimmen Sie die Inhalte und die primitiven Anteile der beiden Polynome!

Lösung: Da alle Koeffizienten gerade sind und X^4 jeweils den Koeffizienten zwei hat, ist der Inhalt in beiden Fällen gleich zwei. Die primitiven Anteile sind dementsprechend $f^* = \frac{1}{2}f = X^4 + 3X^3 - 15X^2 + 16X - 12$ und $g^* = \frac{1}{2}g = X^4 - 2X^2 - 3X - 2$.

b) Bestimmen Sie den ggT mit führendem Koeffizienten eins von $f \bmod 5$ und $g \bmod 5$ in $\mathbb{F}_5[X]$!

Lösung: Wir wenden den EUKLIDischen Algorithmus an; alle Rechenoperationen werden in $\mathbb{F}_5[X]$ ausgeführt. Modulo fünf haben f und g die Repräsentanten $2X^4 + X^3 + 2X + 1$ und $2X^4 + X^2 + 4X + 1$.

$$\begin{aligned}(2X^4 + X^3 + 2X + 1) : (2X^4 + X^2 + 4X + 1) &= 1 \text{ Rest } X^3 + 4X^2 + 3X\\ (2X^4 + X^2 + 4X + 1) : (X^3 + 4X^2 + 3X) &= 2X + 2 \text{ Rest } 2X^2 + 3X + 1\\ (X^3 + 4X^2 + 3X) : (2X^2 + 3X + 1) &= 3X \text{ Rest } 0\end{aligned}$$

Damit liefert uns EUKLID $2X^2 + 3X + 1$ als ggT. Wir suchen den ggT mit führendem Koeffizienten eins; da $2 \cdot 3 \equiv 1 \bmod 5$ ist, müssen wir noch mit drei multiplizieren und erhalten das Ergebnis $X^2 + 4X + 3X$.

c) Bestimmen Sie den ggT mit führendem Koeffizienten eins von $f \bmod 7$ und $g \bmod 7$ in $\mathbb{F}_7[X]$!

Lösung: Jetzt wird eine analoge Rechnung modulo 7 ausgeführt. Für die Inversenbildung beachte man, daß $2 \cdot 4 \equiv 3 \cdot 5 \equiv 1 \bmod 7$ ist.

$$\begin{aligned}(2X^4 + 6X^3 + 5X^2 + 4X + 4) : (2X^4 + 3X^2 + X + 3) &= 1 \text{ Rest } 6X^3 + 2X^2 + 3X + 1\\ (2X^4 + 3X^2 + X + 3) : (6X^3 + 2X^2 + 3X + 1) &= 5X + 3 \text{ Rest } 3X^2 + X\\ (6X^3 + 2X^2 + 3X + 1) : (3X^2 + X) &= 2X \text{ Rest } 3X + 1\\ (3X^2 + X) : (3X + 1) &= X \text{ Rest } 0\end{aligned}$$

Somit ist $3X + 1$ ein ggT; um den mit führendem Koeffizienten eins zu bekommen, müssen wir mit fünf multiplizieren und erhalten $X + 5$.

d) Was können Sie auf Grund der bisherigen Ergebnisse *sicher* über den Grad des ggT von f und g in $\mathbb{Z}[X]$ aussagen?

Lösung: Weder fünf noch sieben teilen beide führenden Koeffizienten; daher ist der Grad des gesuchten ggT höchstens gleich dem des modularen. Der ggT hat also höchstens den Grad eins; er könnte aber auch Grad Null haben.

e) Erraten Sie den ggT von f und g in $\mathbb{Q}[X]$ und beweisen Sie, daß Sie richtig geraten haben!

Lösung: Wenn der ggT linear ist, muß er modulo sieben kongruent zu $X+5$ sein. $X+5$ teilt allerdings keines der beiden Polynome, denn sonst müßte der konstante Koeffizient jeweils durch fünf teilbar sein. Tatsächlich sind die konstanten Koeffizienten der primitiven Anteile -12 und -2; dies spricht eher für $X-2$ als ggT. Einsetzen zeigt, daß beide Polynome an der Stelle zwei verschwinden; daher ist der ggT in $\mathbb{Q}[X]$ gleich $X-2$.

f) Bestimmen Sie den ggT von f und g in $\mathbb{Z}[X]$!

Lösung: Jetzt müssen wir noch die Inhalte der Polynome betrachten; da beide Polynome Inhalt zwei haben, ist der ggT $2(X-2)=2X-4$.

Aufgabe 2: *(8 Punkte)*
Hier seien $f=6X^2-7X-3$ und $g=2X^2-5X+2$.

a) Für welche Primzahlen p können Sie anhand der bislang vorliegenden Information nicht ausschließen, daß der ggT von f und g in $\mathbb{Z}[X]$ einen größeren Grad hat als der von $f \bmod p$ und $g \bmod p$ in $\mathbb{F}_p[X]$?

Lösung: Wenn der ggT von f und g einen größeren Grad hat als der von $f \bmod p$ und $g \bmod p$, muß p den führenden Koeffizienten sowohl von f als auch von g teilen. Dies ist nur für $p=2$ der Fall; hier kann der modulare ggT eventuell einen kleineren Grad haben als der ggT in $\mathbb{Z}[X]$.

b) Berechnen Sie die Resultante der beiden Polynome $f=6X^2-7X-3$ und $g=2X^2-5X+2$ aus $\mathbb{Z}[X]$!

Lösung:

$$\operatorname{Res}(f,g)=\begin{vmatrix}6&-7&-3&0\\0&6&-7&-3\\2&-5&2&0\\0&2&-5&2\end{vmatrix}=6\begin{vmatrix}6&-7&-3\\-5&2&0\\2&-5&2\end{vmatrix}+2\begin{vmatrix}-7&-3&0\\6&-7&-3\\2&-5&2\end{vmatrix}$$
$$=6\cdot(6\cdot2\cdot2-3\cdot5\cdot5-7\cdot5\cdot2+3\cdot2\cdot2)+2\cdot(7\cdot7\cdot2+3\cdot3\cdot2+7\cdot3\cdot5+3\cdot6\cdot2)$$
$$=6\cdot(24-75-70+12)+2\cdot(98+18+105+36)=6\cdot(-109)+2\cdot257=-140$$

c) Bestimmen Sie den ggT von f und g in $\mathbb{Z}[X]$!

Lösung: Da die Resultante nicht verschwindet, haben die beiden Polynome keinen gemeinsamen Faktor positiven Grades. Da sie primitiv sind, ist ihr ggT daher eins.

d) Für welche Primzahlen p hat $\operatorname{ggT}(f \bmod p, g \bmod p)$ einen größeren Grad als $\operatorname{ggT}(f,g)$?

Lösung: $140=2^2\cdot5\cdot7$. Da $f \bmod 2=X+1$ und $g \bmod 2=X$ kleineren Grad als f und g haben, ist $\operatorname{Res}_X(f \bmod 2, g \bmod 2)$ eine andere Determinante als $\operatorname{Res}_X(f,g) \bmod 2$, und in der Tat ist der modulare ggT gleich eins. 5 und 7 teilen keinen der führenden Koeffizienten; daher haben für $p=5$ oder 7 die modularen Polynome einen gemeinsamen Faktor positiven Grades, so daß der Grad des modularen ggT größer ist als der Grad Null des ggT in $\mathbb{Z}[X]$.

e) g hat die beiden Nullstellen 2 und $\frac{1}{2}$. Bestimmen Sie die L^1-Norm, die L^2-Norm, die Höhe und das Maß von g!

Lösung: g hat die L^1-Norm $2+5+2=9$ und die L^2-Norm $\sqrt{2^2+5^2+2^2}=\sqrt{33}$. Die Höhe ist der größte Betrag eines Koeffizienten, also fünf. Das Maß ist der führende Koeffizient zwei mal für jede Nullstelle vom Betrag größer eins deren Betrag, also $2\cdot2=4$.

Aufgabe 3: *(12 Punkte)*

Für das Polynom $f = X^4 - 10X^3 + 25X^2 - 20X + 4$ ist $f \equiv (X^2+2X+2)(X^2+3X+2) \bmod 5$.

a) Setzen Sie diese Faktorisierung modulo fünf nach dem HENSELschen Lemma fort zu einer Faktorisierung modulo fünfundzwanzig!

Lösung: Sei $g_0 = X^2+2X+2$ und $h_0 = X^2+3X+2$. Gesucht sind Polynome $g_1, h_1 \in \mathbb{Z}[X]$ vom Grad höchstens zwei derart, daß gilt

$$(g_0 + 5g_1)(h_0 + 5h_1) = g_0h_0 + 5(g_0h_1 + h_0g_1) + 25g_1h_1 \equiv f \bmod 25\,.$$

Konkret ist

$$\begin{aligned} f - g_0h_0 &= (X^4 - 10X^3 + 25X^2 - 20X + 4) - (X^4 + 5X^3 + 10X^2 + 10X + 4) \\ &= -15X^3 + 15X^2 - 30X = 5 \cdot (-3X^3 + 3X^2 - 6X)\,; \end{aligned}$$

die obige Kongruenz gilt also genau dann, wenn $g_0h_1 + h_0g_1 \equiv -3X^3 + 3X^2 - X \bmod 5$.
Als erster Schritt zur Berechnung von g_1 und h_1 wird der erweiterte EUKLIDische Algorithmus angewendet auf g_0 und h_0:

$$(X^2 + 2X + 2) : (X^2 + 3X + 2) = 1 \text{ Rest } -X \Longrightarrow -X = g_0 - h_0$$
$$(X^2+3X+2) : (-X) = -X-3 \text{ Rest } 2 \Longrightarrow 2 = h_0 + (X+3)(g_0 - h_0) = (X+3)g_0 - (X+2)h_0\,.$$

Wegen $2 \cdot 3 \equiv 1 \bmod 5$ ist somit $1 = (3X+4)g_0 - (3X+1)h_0$ in $\mathbb{F}_5[X]$.
Multiplikation mit $(f - g_0h_0)/5$ macht daraus

$$-3X^3 + 3X^2 - X \equiv (X^4 + 2X^3 + 4X^2 + X)g_0 - (X^4 + X^3 + 4X)h_0 \bmod 5\,.$$

Davon können (und müssen) wir zur Gradreduktion noch ein geeignetes Vielfaches der Gleichung $h_0g_0 - g_0h_0 = 0$ subtrahieren. Dazu dividieren wir den Faktor vor g_0 durch h_0:

$$(X^4 + 2X^3 + 4X^2 + X) : (X^2 + 3X + 2) = X^2 + 4X \text{ Rest } 3X\,.$$

Wir probieren es daher mit dem $(X^2 + 4X)$-fachen. Der Koeffizient vor h_0 wird dann zu $(X^4 + X^3 + 4X) - (X^2 + 4X)g_0 = X$, und der vor g_0 zum obigen Divisionsrest $3X$. Somit ist

$$-3X^3 + 3X^2 - X \equiv 3X \cdot g_0 - X \cdot h_0 \bmod 5\,.$$

Wir können also $h_1 = 3X$ und $g_1 = -X = 4X$ setzen. Damit wird

$$f \equiv (g_0 + 5g_1)(h_0 + 5h_1) = (X^2 + 22X + 2)(X^2 + 18X + 2) \bmod 25\,.$$

Ausmultiplizieren zeigt, daß in der Tat $f - (g_0 + 5g_1)(h_0 + 5h_1) = -50X^3 - 375X^2 - 100X$ durch 25 teilbar ist.

b) Finden Sie damit eine Zerlegung von f in $\mathbb{Z}[X]$ als Produkt zweier quadratischer Polynome!

Lösung: Wie die Probe am Ende von Teil *a)* zeigte, können wir die Faktoren nicht einfach so übernehmen. Da f nur recht kleine Koeffizienten hat, könnten wir versuchen, die doch recht großen Koeffizienten von X in beiden Polynomen um 25 zu vermindern. Damit wird

$$(X^2 - 3X + 2)(X^2 - 7X + 2) = X^4 - 10X^3 + 25X^2 - 20X + 4\,,$$

und das ist unser Ausgangspolynom f.

c) Zeigen Sie, daß eines dieser Polynome in $\mathbb{Z}[X]$ irreduzibel ist, während das andere als Produkt zweier Linearfaktoren aus $\mathbb{Z}[X]$ geschrieben werden kann.

Lösung: Wenn sich eines dieser Polynome als Produkt von Linearfaktoren aus $\mathbb{Z}[X]$ schreiben läßt, ist es wegen des führenden Koeffizienten eins ein Produkt der Form $(X-a)(X-b)$.

Dann ist ab gleich dem konstanten Term, und $-a-b$ gleich dem Koeffizienten von X. Offensichtlich gibt es keine ganzen Zahlen mit Produkt zwei und Summe sieben; daher ist X^2-7X+2 irreduzibel. Ganze Zahlen mit Produkt zwei und Summe drei sind eins und zwei; also ist $X^2-3X+2=(X-1)(X-2)$.

d) Wie sieht die Zerlegung von f in ein Produkt irreduzibler Faktoren in $\mathbb{Z}[X]$ und in $\mathbb{Q}[X]$ aus?

Lösung: Da alle betrachteten Faktoren primitiv sind, sind sie nach GAUSS genau dann irreduzibel in $\mathbb{Q}[X]$, wenn sie in $\mathbb{Z}[X]$ irreduzibel sind. In beiden Polynomringen ist daher $f=(X-1)(X-2)(X^2-7X+2)$ die gesuchte Zerlegung.

Aufgabe 4: *(10 Punkte)*
Welche der folgenden Teilmengen sind auch Ideale des jeweiligen Rings?

a) $\{z\in\mathbb{Z}\mid 2z\equiv 3 \bmod 5\}\subset\mathbb{Z}$

Lösung: Sind $2z\equiv 2w\equiv 3 \bmod 5$, so ist $2(z+w)\equiv 1 \bmod 5$, d.h. die Summe zweier Elemente liegt nicht mehr in der Menge. Somit kann diese kein Ideal sein.

b) $\{z\in\mathbb{Z}\mid z \text{ gerade}\}\subset\mathbb{Z}$

Lösung: Da die Summe zweier gerader Zahlen wieder gerade ist und das Produkt einer beliebigen ganzen Zahl mit einer geraden Zahl auch, ist dies ein Ideal, genauer: Es ist das Hauptideal (2).

c) $\{f\in\mathbb{Q}[X]\mid f \text{ hat eine mindestens doppelte Nullstelle bei } x=1\}\subset\mathbb{Q}[X]$

Lösung: f hat eine mindestens doppelte Nullstelle bei $x=1$ genau dann, wenn f in $\mathbb{Q}[X]$ durch $(X-1)^2$ teilbar ist. Somit ist diese Menge gleich dem Hauptideal $\big((X-1)^2\big)$.

d) $\left\{f=\sum\limits_{i=0}^{d}a_iX^i \mid d\in\mathbb{N}_0,\ a_i\in\mathbb{Z} \text{ und } \sum\limits_{i=0}^{d}a_i=0\right\}\subset\mathbb{Z}[X]$

Lösung: Die Summe der Koeffizienten ist gleich $f(1)$; die Teilmenge ist daher der Kern des Homomorphismus $\mathbb{Z}[X]\to\mathbb{Z}$, der jedes Polynom f auf den Wert $f(1)$ abbildet. Als Kern eins Homomorphismus ist sie natürlich ein Ideal.

e) $\{f\in\mathbb{R}[X,Y]\mid f(x,y)=f(y,x) \text{ für alle } x,y\in\mathbb{R}\}\subset\mathbb{R}[X,Y]$

Lösung: Dies ist kein Ideal, denn zwar liegt beispielsweise $X+Y$ in der Teilmenge, nicht aber das Produkt $X(X+Y)=X^2+XY$, denn es verschwindet an der Stelle $(0,1)$, nimmt bei $(1,0)$ aber den Wert eins an.

Aufgabe 5: *(10 Punkte)*

a) Bringen Sie die Terme des Polynoms $f=2X^3Y+2XY^3+2X-X^2Y-Y^3-2+Y$ in die Reihenfolge, die der graduiert lexikographischen Ordnung mit $X>Y$ entspricht!

Lösung: $f=2X^3Y+2XY^3-X^2Y-Y^3+2X+Y-2$

b) Dividieren Sie f bezüglich dieser Ordnung durch die beiden Polynome $f_1=X^2Y+Y^3+2$ und $f_2=Y^2X+X^3+1$!

Lösung: Der führende Term von f_1 ist X^2Y, der von f_2 ist X^3. Der führende Term von f ist durch X^2Y teilbar, also wird $2Xf_1$ von f subtrahiert; übrig bleibt $-X^2Y-Y^3-2X+Y-2$.

Wieder ist der führende Term durch X^2Y teilbar; also wird f_1 addiert, was auf $-2X+Y$ führt. Keiner der verbleibenden Terme ist durch einen führenden Term von f_1 oder f_2 teilbar. Also ist $f = (2X-1)f_1 + (-2X+Y)$.

c) Können Sie eine Aussage treffen, ob f im Ideal $I = (f_1, f_2)$ des Polynomrings $\mathbb{Q}[X, Y]$ liegt?

Lösung: Da der Divisionsrest von Null verschieden ist, konnte nicht gezeigt werden, daß f im Ideal (f_1, f_2) liegt. Andererseits kann bei der Division durch eine Menge, die keine GRÖBNER-Basis ist, ein Divisionsrest ungleich Null auftreten, obwohl der Dividend im Ideal liegt. Wir können also keine sichere Aussage machen.

d) Zeigen Sie, daß die Polynome $g_1 = 2X - Y$ und $g_2 = 5Y^3 + 8$ eine GRÖBNER-Basis des Ideals (g_1, g_2) bezüglich der graduiert lexikographischen Ordnung bilden!

Lösung: Die führenden Monome X und Y^3 sind teilerfremd; daher läßt sich $S(g_1, g_2)$ modulo $\{g_1, g_2\}$ auf Null reduzieren, so daß g_1 und g_2 nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis bilden.

e) Tatsächlich ist $I = (g_1, g_2)$. (Das müssen Sie nicht zeigen.) Können Sie mit dieser Zusatzinformation entscheiden, ob f in I liegt?

Lösung: Der Divisionsrest in *b)* war $-g_1$; somit ist $f = (2X-1)f_1 - g_1 \in I$, da f_1 und g_1 beide in I liegen.

Aufgabe 6: *(10 Punkte)*

k sei ein Körper, und I ein Ideal im Polynomring $k[X, Y, Z]$.

a) Wie ist eine Monomordnung auf diesem Polynomring definiert?

Lösung: Sie muß eine Totalordnung sein, d.h. für zwei Monome $X^aY^bZ^c$ und $X^\alpha Y^\beta Z^\gamma$ muß genau eine der drei Beziehungen $X^aY^bZ^c = X^\alpha Y^\beta Z^\gamma$, $X^aY^bZ^c < X^\alpha Y^\beta Z^\gamma$ oder $X^aY^bZ^c > X^\alpha Y^\beta Z^\gamma$ gelten.

Außerdem muß aus $X^aY^bZ^c < X^\alpha Y^\beta Z^\gamma$ folgen, daß für jedes Monom $X^\ell Y^m Z^n$ auch gilt $X^{a+\ell}Y^{b+m}Z^{c+n} < X^{\alpha+\ell}Y^{\beta+m}Z^{\gamma+n}$.

Schließlich muß es sich noch um eine Wohlordnung handeln, d.h. jede Menge von Monomen hat ein kleinstes Element.

b) Wie ist eine GRÖBNER-Basis von I definiert?

Lösung: Eine GRÖBNER-Basis ist eine endliche Teilmenge von I mit der Eigenschaft, daß die führenden Monome ihrer Elemente das Ideal $\operatorname{FM} I$ erzeugen, das von den führenden Monomen *aller* Polynome aus I erzeugt wird.

c) Hat jedes Ideal I bezüglich jeder Monomordnung eine GRÖBNER-Basis?

Lösung: Ja; das ist der Satz von BUCHBERGER.

d) Zeigen Sie, daß das Polynom $f = X^2 + 2Y^2 + 3Z + 5X^2Y^2Z^2 + 7XY + 11YZ$ bezüglich jeder Monomordnung denselben führenden Term hat, und bestimmen Sie diesen!

Lösung: Alle vorkommenden Monome sind Teiler von $X^2Y^2Z^2$, und bezüglich jeder Monomordnung sind echte Teiler eines Monoms kleiner als dieses. Somit ist $5X^2Y^2Z^2$ bezüglich jeder Monomordnung der führende Term.

e) Zeigen Sie, daß die beiden Polynome $g_1 = X^5 + X^4Y + Y^6 + Z^4 + X^2Y^2Z^2 + X^3Y^4$ und $g_2 = X^5 + Z^6 + X^2Y^3 + XYZ$ bezüglich der graduiert lexikographischen Ordnung eine GRÖBNER-Basis des von ihnen erzeugten Ideals bilden!

Lösung: $\mathrm{FM}\, g_1 = X^3Y^4$ und $\mathrm{FM}\, g_2 = Z^6$ sind zueinander teilerfremd; daher läßt sich $S(g_1, g_2)$ modulo $\{g_1, g_2\}$ auf Null reduzieren, so daß die beiden Polynome nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis bilden.

Aufgabe 7: *(10 Punkte)*

a) Bestimmen Sie die reduzierte GRÖBNER-Basis bezüglich der lexikographischen Ordnung für das von den Polynomen $f = X^2 - 4X + Y^2 + 2$ und $g = 2X^2 - 8X + 3Y^2 + 3$ in $\mathbb{Q}[X, Y]$ erzeugte Ideal I!

Lösung: Das führende Monom ist jeweils X^2; daher ist $h = 2S(f, g) = 2f - g = -Y^2 + 1$. Dieses Polynom läßt sich durch den Divisionsalgorithmus nicht weiter reduzieren, da keines seiner Monome durch X^2 teilbar ist. Somit muß h nach dem BUCHBERGER-Algorithmus zum Erzeugendensystem dazu genommen werden. $S(f, h)$ und $S(g, h)$ lassen sich auf Null reduzieren, da die führenden Monome X^2 und Y^2 teilerfremd sind; also bilden f, g, h eine GRÖBNER-Basis. Da $\mathrm{FM}\, f = \mathrm{FM}\, g$, können wir auf eines dieser Polynome verzichten, d.h. auch f und h bilden eine GRÖBNER-Basis. Wenn wir eine reduzierte Basis wollen, müssen wir den führenden Term von h auf eins normieren, d.h. h ersetzen durch $-h$. Das führende Monom Y^2 kommt auch in f vor; daher muß f ersetzt werden durch $f+h = X^2-4X+3$. Die reduzierte GRÖBER-Basis besteht also aus den beiden Polynomen $Y^2 - 1$ und $X^2 - 4X + 3$.

b) Hat diese GRÖBNER-Basis eine Form gemäß dem *Shape*-Lemma?

Lösung: Nein; wir haben zwei Polynome in jeweils nur einer Veränderlichen, während eine Basis nach dem *Shape*-Lemma aus einem Polynom nur in Y und einen in X linearen Polynom aus $\mathbb{Q}[X, Y]$ bestehen müßte.

c) Finden Sie eine $\mathbb{Q}$-Vektorraumbasis von $\mathbb{Q}[X, Y]/I$!

Lösung: Eine solche Basis bilden die Standardmonome, d.h. die Monome, die weder durch $\mathrm{FM}\, f = X^2$ noch durch $\mathrm{FM}\, h = Y^2$ teilbar sind. Es sind die vier Monome $1, X, Y$ und XY.

d) Bestimmen Sie die Nullstellenmenge $V_{\mathbb{C}}(I)$!

Lösung: $Y^2 - 1$ verschwindet an den Stellen $y = \pm 1$, und $X^2 - 4X + 3 = (X - 2)^2 - 1$ hat die Nullstellen $x = 1$ und $x = 3$. Somit ist $V_{\mathbb{C}}(I) = \big\{(1, 1),\ (1, -1),\ (3, 1),\ (3, -1)\big\}$.

e) Interpretieren Sie diese geometrisch!

Lösung: $f = X^2 - 4X + Y^2 + 2 = (X - 2)^2 + Y^2 - 2$ hat als Nullstellenmenge den Kreis im $(2, 0)$ mit Radius $\sqrt{2}$, und $g = 2X^2 - 8X + 3Y^2 + 3 = 2(X - 2)^2 + 3Y^2 - 5$ eine Ellipse. Die beiden schneiden sich in den vier berechneten Punkten.

f) Welche Vielfachheiten haben die gefundenen Nullstellen jeweils?

Lösung: Alle Nullstellen sind einfach, denn es gibt vier Stück, und die Dimension von $\mathbb{Q}[X, Y]$ ist ebenfalls vier. Da diese Dimension gleich der Summe der Vielfachheiten ist, müssen alle gleich eins sein.

g) Finden Sie dazu eine separierende Linearform aus $\mathbb{Q}[X, Y]$!

Lösung: Beispielsweise nimmt $X + 2Y$ auf der Nullstellenmenge die vier verschiedenen Werte 3, -1, 5 und 1 an.

h) Ist I ein Radikalideal?

Lösung: Ja, denn alle Nullstellen sind einfach.