Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie
Prof. Marc Nieper-Wißkirchen

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 5 zur Algebra I

Abgabe bis 22. Mai 2013, 12:00 Uhr

Aufgabe 1. *Elementarsymmetrische Funktionen*

a) Gib $e_2(X, Y, Z, U, V)$, also die zweite elementarsymmetrische Funktion in den fünf Unbestimmten X, Y, Z, U und V, explizit an.

b) Schreibe $X^2 + Y^2 + Z^2$ als polynomiellen Ausdruck in den $e_i(X, Y, Z)$.

c) Schreibe $X_1^2 + \cdots + X_n^2$ als polynomiellen Ausdruck in den $e_i(X_1, \ldots, X_n)$.

d) Zeige, dass $e_k(\underbrace{1, \ldots, 1}_{n \text{ Argumente}}) = \binom{n}{k}$.

Lösung.

a) $e_2(X, Y, Z, U, V) = XY + XZ + XU + XV + YZ + YU + YV + ZU + ZV + UV.$

b) $X^2 + Y^2 + Z^2 = (X + Y + Z)^2 - 2\,XY - 2\,XZ - 2\,YZ = e_1(X, Y, Z)^2 - 2\,e_2(X, Y, Z).$

c) $X_1^2 + \cdots + X_n^2 = (X_1 + \cdots + X_n)^2 - 2 \sum_{1 \le i < j \le n} X_i X_j = e_1(X_1, \ldots, X_n)^2 - 2\,e_2(X_1, \ldots, X_n).$

d) *Variante 1:* $e_k(1, \ldots, 1) = \sum_{1 \le i_1 < \cdots < i_k \le n} 1 = \binom{n}{k}$, denn der Summand 1 wird genau so oft summiert, wie es Möglichkeiten gibt, aus den Zahlen $\{1, \ldots, n\}$ genau k Stück als Indizes auszuwählen.

Variante 2: Vielleicht kennt man die Formel

$$\prod_{i=1}^{n} (1 + X_i\,T) = \sum_{k=0}^{n} e_k(X_1, \ldots, X_n)\,T^k.$$

Setzt man in dieser Identität alle X_i auf 1, folgt die Behauptung sofort mit dem binomischen Lehrsatz

$$\prod_{i=1}^{n} (1 + T) = (1 + T)^n = \sum_{k=0}^{n} \binom{n}{k} T^k$$

und Koeffizientenvergleich.

Variante 2': Auf ähnliche Art und Weise kann man auch die Formel

$$\prod_{i=1}^{n} (T + X_i) = \sum_{k=0}^{n} e_{n-k}(X_1, \ldots, X_n)\,T^k$$

als Ausgangspunkt verwenden. Deren Vorteil ist, dass man ihre Korrektheit ganz mühelos beweisen kann: Denn die linke Seite der Gleichung hat – als Polynom in der einzigen Variablen T mit Koeffizienten aus $\mathbb{Q}[X_1, \ldots, X_n]$ gedacht – die Nullstellen $-X_1, \ldots, -X_n$. Daher liefert der Vietasche Satz sofort die Behauptung.

Variante 3': Variante 2' kann man etwas expliziter auch wie folgt formulieren. Das Polynom $(1 + T)^n = \sum_{k=0}^{n} \binom{n}{k} T^{n-k}$ hat die Zahl -1 als n-fache Nullstelle. Mit dem Vietaschen Satz folgt daher

$$k\text{-ter Koeffizient} = \binom{n}{n-k} = (-1)^{n-k} e_{n-k}(-1, \ldots, -1) = e_{n-k}(1, \ldots, 1).$$

Variante 3: Analog kann man Variante 2 explizit ausführen: Das Polynom $(T-1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k T^{n-k}$ hat die Zahl $+1$ als n-fache Nullstelle. Mit dem Vietaschen Satz folgt daher

$$k\text{-ter Koeff.} = (-1)^{n-k}\binom{n}{n-k} = (-1)^{n-k}(-1)^{n-k} e_{n-k}(1,\dots,1) = e_{n-k}(1,\dots,1).$$

Aufgabe 2. *Der Vietasche Satz*

a) Sei $X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = 0$ eine normierte Polynomgleichung vierten Grades, deren Lösungen mit Vielfachheiten x_1, x_2, x_3 und x_4 seien. Drücke die Koeffizienten a_0, a_1, a_2 und a_3 explizit als Polynome in den x_i aus.

b) Verwende den Vietaschen Satz für $n = 2$ um die bekannte Lösungsformel für normierte quadratische Gleichungen herzuleiten.

Lösung.

a) Wir multiplizieren $(X - x_1)\cdots(X - x_4)$ aus und führen einen Koeffizientenvergleich durch. Damit folgen die gesuchten Beziehungen:

$$\begin{aligned}
a_0 &= e_4(x_1,\dots,x_4) = x_1x_2x_3x_4 \\
a_1 &= -e_3(x_1,\dots,x_4) = -(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) \\
a_2 &= e_2(x_1,\dots,x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
a_3 &= -e_1(x_1,\dots,x_4) = -(x_1 + x_2 + x_3 + x_4) \\
1 &= e_0(x_1,\dots,x_4)
\end{aligned}$$

Bemerkung: Wenn man den Vietaschen Satz zitiert, kann man sich das Ausmultiplizieren sparen.

b) Sei $X^2 + bX + c = 0$ eine allgemeine normierte quadratische Gleichung und seien x_1, x_2 ihre (nach dem Fundamentalsatz der Algebra existierenden) komplexen Lösungen (mit Vielfachheiten). Ausmultiplizieren von $(X - x_1)(X - x_2)$ und Koeffizientenvergleich führt zu den Beziehungen

$$\begin{aligned}
c &= x_1x_2, \\
b &= -(x_1 + x_2),
\end{aligned}$$

wie vom Vietaschen Satz vorausgesagt. Dann gibt es zwei Möglichkeiten fortzufahren:

Variante 1 (tatsächliche Herleitung): Mit den Beziehungen können wir den (aus der Schule bekannten) Ausdruck für die Determinante herleiten, denn

$$\Delta = (x_1 - x_2)^2 = x_1^2 + 2x_1x_2 + x_2^2 - 4x_1x_2 = b^2 - 4c.$$

Somit gilt

$$x_1 - x_2 = \pm\sqrt{\Delta},$$

wobei das „$\pm$"-Zeichen hier bedeuten soll, dass für *eine* der beiden komplexen Wurzeln von Δ die Gleichung stimmt. Über einen üblichen Trick, den wir etwa schon bei den Formeln für Real- und Imaginärteil komplexer Zahlen gesehen haben, folgt:

$$\begin{aligned}
x_1 &= \frac{(x_1 + x_2) + (x_1 - x_2)}{2} = \frac{-b \pm \sqrt{\Delta}}{2} \\
x_2 &= \frac{(x_1 + x_2) - (x_1 - x_2)}{2} = \frac{-b \mp \sqrt{\Delta}}{2}
\end{aligned}$$

Variante 2 (lediglich Verifikation): Alternativ können wir uns damit begnügen, die bekannte Formel zu verifizieren:

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{x_1 + x_2 \pm \sqrt{(x_1 - x_2)^2}}{2} = \frac{x_1 + x_2 \pm (x_1 - x_2)}{2} = x_1 \text{ bzw. } x_2.$$

Bemerkung: Dem ersten Anschein nach haben wir hier die Rechenregel „$\sqrt{a^2} = a$“ verwendet, die ja völlig falsch ist – für reelle a gilt stattdessen $\sqrt{a^2} = |a|$, und für komplexe a sollte man lieber nicht von der Wurzel reden. In der Rechnung wird der Wurzelausdruck allerdings von einem „$\pm$“-Zeichen geschützt; dann ist das okay (wieso?).

Aufgabe 3. *Diskriminanten kubischer Gleichungen*

a) Finde eine normierte Polynomgleichung dritten Grades, welche 1 als zweifache Lösung, 2 als einfache Lösung und keine weiteren Lösungen besitzt. Was ist ihre Diskriminante?

b) Sei $X^3 + pX + q = 0$ eine allgemeine reduzierte kubische Gleichung. Zeige, dass ihre Diskriminante durch $-4p^3 - 27q^2$ gegeben ist.

Lösung.

a) $(X-1)^2(X-2) = 0$ tut's. Ihre Diskriminante ist 0, da sie ja doppelte Lösungen besitzt.

   Bemerkung: Ausmultipliziert lautet die Gleichung $X^3 - 4\,X^2 + 5\,X - 2 = 0$.

b) *Variante 1 (lange Rechnung mit Tricks):* Seien x, y, z die drei Lösungen der Gleichung. Der Vietasche Satz liefert die Beziehungen

$$\begin{aligned} 0 &= x + y + z, \\ p &= xy + xz + yz, \\ q &= -xyz. \end{aligned}$$

Daher folgt

$$\begin{aligned} \Delta &= (x-y)^2 \cdot (x-z)^2 \cdot (y-z)^2 \\ &= (x^2 + 2xy + y^2 - 4xy) \cdot (x^2 + 2xz + z^2 - 4xz) \cdot (y^2 + 2yz + z^2 - 4yz) \\ &= ((x+y)^2 - 4xy) \cdot ((x+z)^2 - 4xz) \cdot ((y+z)^2 - 4yz) \\ &= (z^2 - 4xy) \cdot (y^2 - 4xz) \cdot (x^2 - 4yz) \\ &= -63x^2y^2z^2 - 4x^3y^3 - 4x^3z^3 - 4y^3z^3 + 16x^4yz + 16xy^4z + 16xyz^4 \\ &= -63x^2y^2z^2 - 4(x^3y^3 + x^3z^3 + y^3z^3) + 16xyz(x^3 + y^3 + z^3) \\ &= \text{(weitere Tricks)} \\ &= -4p^3 - 27q^2. \end{aligned}$$

Variante 2 (lange Rechnung ohne Tricks): Seien wieder x, y, z die drei Lösungen der Gleichung. Wegen der obigen Beziehungen können wir $z = -x - y$ schreiben; dann folgt

$$\begin{aligned} \Delta &= (x-y)^2 \cdot (x-z)^2 \cdot (y-z)^2 \\ &= (x-y)^2 \cdot (2x+y)^2 \cdot (x+2y)^2 \\ &= 4y^6 + 12xy^5 - 3x^2y^4 - 26x^3y^3 - 3x^4y^2 + 12x^5y + 4x^6 \end{aligned}$$

$$\begin{aligned} -4p^3 - 27q^2 &= -4 \cdot (-x^2 - xy - y^2)^3 - 27 \cdot (xy^2 + x^2y) \\ &= 4y^6 + 12xy^5 - 3x^2y^4 - 26x^3y^3 - 3x^4y^2 + 12x^5y + 4x^6, \end{aligned}$$

also stimmen die beiden Seiten der zu zeigenden Gleichung überein.

Variante 3 (durch Überlegung): Aus der Vorlesung ist bereits bekannt, dass die Diskriminante Δ auf genau eine Art und Weise ein polynomieller Ausdruck in den Koeffizienten p und q (und 0) der Gleichung ist. Da p vom Grad 2, q vom Grad 3 und Δ vom Grad 6 in den Nullstellen ist, gibt es für die Gestalt dieses Ausdrucks nur eine Möglichkeit, nämlich

$$\Delta = \alpha p^3 + \beta q^2,$$

wobei die konstanten Vorfaktoren noch zu bestimmen sind. Da diese für jede reduzierte kubische Gleichung gleich sind (sie sind universelle Konstanten), können wir diese dadurch bestimmen, indem wir bestimmte einfache Beispielgleichungen betrachten:

1. Die Gleichung $X^3 - X = 0$ hat $p = -1$, $q = 0$ und die drei Lösungen $-1, 0, 1$. Ihre Diskriminante ist 4. Also folgt aus $4 = \Delta = \alpha \cdot (-1)^3$, dass $\alpha = -4$ sein muss.

2. Die Gleichung $X^3 - 3\,X + 2 = 0$ hat $p = -3$, $q = 2$ und die drei Lösungen $1, 1, -2$. Ihre Diskriminante ist 0. Also folgt aus $0 = \Delta = -4 \cdot (-3)^3 + \beta \cdot 2^2$, dass $\beta = -27$ sein muss.

2.' *(alternativ)* Die Gleichung $X^3 - 1 = 0$ hat $p = 0$, $q = -1$ und die drei Lösungen $1, \omega, \omega^2$ mit $\omega = \exp(2\pi \mathrm{i}/3)$. Ihre Diskriminante ist -27 – wenn man die Beziehung $\omega^2 = -\omega - 1$, die wir schon in Aufgabe 5 von Blatt 2 gesehen haben, verwendet, ist die Rechnung relativ schmerzlos:

$$\begin{aligned} \Delta &= (1-\omega)^2 \cdot (1-\omega^2)^2 \cdot (\omega - \omega^2)^2 \\ &= (1-\omega)^2 \cdot (2+\omega)^2 \cdot (2\omega+1)^2 \\ &= (1 - 2\omega + \omega^2) \cdot (4 + 4\omega + \omega^2) \cdot (4\omega^2 + 4\omega + 1) \\ &= (-3\omega) \cdot (3 + 3\omega) \cdot (-3) \\ &= 27 \cdot (\omega + \omega^2) \\ &= -27 \end{aligned}$$

   Also folgt $\beta = -27$.

Damit ist die Behauptung bewiesen.

Bemerkung (danke an Mirjam Fahrion): Der Grund, wieso in Δ keine niedrigeren Potenzen wie p^1, p^2, q^1 oder gar konstante Glieder auftreten können, ist folgender: Der Ausdruck Δ ist nicht nur irgendein Polynom vom Grad 6 in den Nullstellen, sondern sogar ein *homogenes* Polynom vom Grad 6 in den Nullstellen, d. h. alle vorkommenden Monome haben jeweils Grad 6.

Aufgabe 4. *Symmetrien eines Polynoms*

Sei $f(X, Y, Z, W) := XY+ZW+XYZW$. Wie viele vierstellige Permutationen σ mit $\sigma \cdot f = f$ gibt es?

Lösung. *Variante 1:* Man kann alle 24 vierstelligen Permutationen σ durchgehen und jeweils $\sigma \cdot f$ mit f vergleichen:

$xyzw$	$xy + zw + xyzw$	
$xyzw$	$xy + zw + xyzw$	✓
$wxyz$	$xw + yz + xyzw$	
$xwyz$	$xw + yz + xyzw$	
$xywz$	$xy + zw + xyzw$	✓
$xzyw$	$xz + yw + xyzw$	
$wxzy$	$xw + yz + xyzw$	
$xwzy$	$xw + yz + xyzw$	
$xzwy$	$xz + yw + xyzw$	
$yxzw$	$xy + zw + xyzw$	✓
$wyxz$	$xz + yw + xyzw$	
$ywxz$	$xz + yw + xyzw$	
$yxwz$	$xy + zw + xyzw$	✓
$yzxw$	$xw + yz + xyzw$	
$wyzx$	$xz + yw + xyzw$	
$ywzx$	$xz + yw + xyzw$	
$yzwx$	$xw + yz + xyzw$	
$wzxy$	$xy + zw + xyzw$	✓
$zxyw$	$xz + yw + xyzw$	
$zwxy$	$xy + zw + xyzw$	✓
$zxwy$	$xz + yw + xyzw$	
$wzyx$	$xy + zw + xyzw$	✓
$zyxw$	$xw + yz + xyzw$	
$zwyx$	$xy + zw + xyzw$	✓
$zywx$	$xw + yz + xyzw$	

Also lassen genau acht Permutationen das Polynom invariant.

Variante 2: Der hintere Summand bleibt unter jeder Permutation invariant. Der vordere bleibt unter Vertauschung $x \leftrightarrow y$ (und sowieso $z \leftrightarrow w$) invariant, also unter insgesamt vier Permutationen. Analog ist es für den mittleren Summanden. Außerdem kann man aber noch mittels $x \leftrightarrow z, y \leftrightarrow w$ die beiden Summanden vertauschen; insgesamt gibt es daher acht Permutationen, die das Polynom als Ganzes invariant lassen.

Aufgabe 5. *Formale Ableitung von Polynomen*

a) Seien $g(X)$ und $h(X)$ Polynome. Zeige:

$$(gh)^{(k)}(X) = \sum_{i+j=k} \binom{k}{i} g^{(i)}(X)\, h^{(j)}(X).$$

b) Sei $f(X)$ ein Polynom und n eine natürliche Zahl. Zeige: $f^{(n+1)} = 0 \iff \deg f \leq n$.

c) Sei $f(X)$ ein Polynom und a eine komplexe Zahl. Zeige, dass die Entwicklung von $f(X)$ nach $X - a$ durch die *Taylorsche Formel* gegeben ist (nach Brooke Taylor, 1685–1731, britischer Mathematiker):

$$f(X) = \sum_{k=0}^{\infty} \frac{f^{(k)}(a)}{k!} (X - a)^k$$

Lösung.

a) Wir führen einen Induktionsbeweis über $k \geq 0$. Dabei ist der Induktionsanfang $k = 0$ klar. Für den Induktionsschritt $k \to k+1$ führen wir die Rechnung

$$\begin{aligned}
(gh)^{(k+1)} = ((gh)')^{(k)} = (g'h + gh')^{(k)} &= (g'h)^{(k)} + (gh')^{(k)} \\
&\overset{\text{IV}}{=} \sum_{i+j=k} \binom{k}{i} (g')^{(i)} h^{(j)} + \sum_{i+j=k} \binom{k}{i} g^{(i)} (h')^{(j)} \\
&= \sum_{i+j=k} \binom{k}{i} g^{(i+1)} h^{(j)} + \sum_{i+j=k} \binom{k}{i} g^{(i)} h^{(j+1)} \\
&= \sum_{\substack{\hat\imath+\hat\jmath=k+1 \\ \hat\imath \geq 1}} \binom{k}{\hat\imath - 1} g^{(\hat\imath)} h^{(\hat\jmath)} + \sum_{\substack{\hat\imath+\hat\jmath=k+1 \\ \hat\jmath \geq 1}} \binom{k}{\hat\imath} g^{(\hat\imath)} h^{(\hat\jmath)} \\
&= \sum_{\hat\imath+\hat\jmath=k+1} \binom{k}{\hat\imath - 1} g^{(\hat\imath)} h^{(\hat\jmath)} + \sum_{\hat\imath+\hat\jmath=k+1} \binom{k}{\hat\imath} g^{(\hat\imath)} h^{(\hat\jmath)} \\
&= \sum_{\hat\imath+\hat\jmath=k+1} \left(\binom{k}{\hat\imath - 1} + \binom{k}{\hat\imath} \right) g^{(\hat\imath)} h^{(\hat\jmath)} = \sum_{\hat\imath+\hat\jmath=k+1} \binom{k+1}{\hat\imath} g^{(\hat\imath)} h^{(\hat\jmath)}.
\end{aligned}$$

Dabei haben wir der Übersichtlichkeit halber die Konvention $\binom{n}{-1} = 0$ für alle n und die bekannte Rekursionsgleichung für die Binomialkoeffizienten verwendet.

b) „$\Longrightarrow$“: Da f ein Polynom ist, können wir es als eine gewisse endliche Summe $f = \sum_{i=0}^{m} a_i X^i$ schreiben. Eine kurze Überlegung zeigt, dass die k-te Ableitung des Monoms X^i für $i < k$ null ist und für $i \geq k$ durch

$$(X^i)^{(k)} = \frac{i!}{(i-k)!} X^{i-k}$$

gegeben ist. Daher folgt aus der Voraussetzung

$$0 = f^{(n+1)} = \sum_{i=n+1}^{m} \frac{i!}{(i-(n+1))!} a_i X^i$$

durch Koeffizientenvergleich, dass für jedes $i = n+1, \ldots, m$ der Koeffizient $\frac{i!}{(i-(n+1))!} a_i$ null ist. Also sind alle a_i mit $i \geq n+1$ null; das Polynom f hat also in der Tat Grad $\leq n$.

„$\Longleftarrow$“: Alle in f auftretenden Monome verschwinden bei $(n+1)$-maligem Ableiten.

c) Beide Seiten der Gleichung sind linear in f (wieso?); daher genügt es (wieso?), die Identität für die Spezialfälle $f := X^n$, $n \geq 0$, zu bestätigen. Dies gelingt mithilfe des binomischen Lehrsatzes:

$$\begin{aligned}
\sum_{k=0}^{\infty} \frac{f^{(k)}(a)}{k!} (X-a)^k &= \sum_{k=0}^{\infty} \frac{(X^n)^{(k)}(a)}{k!} (X-a)^k \\
&= \sum_{k=0}^{n} \frac{n!/(n-k)! \cdot a^{n-k}}{k!} (X-a)^k \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} (X-a)^k \\
&= (a + (X-a))^n = X^n = f.
\end{aligned}$$

Elegantere Variante (nach Tim Daffler): Das Polynom $f(X)$ lässt sich als Ausdruck der Form

$$f(X) = b_n(X-a)^n + b_{n-1}(X-a)^{n-1} + \cdots + b_1(X-a) + b_0$$

schreiben, wobei die b_i *nicht* die Koeffizienten von f sind, sondern noch zu bestimmen sind – angeblich gilt $b_k = f^{(k)}(a)/k!$. (Dass eine solche Umschreibung möglich ist, erkennt man, wenn man $f(X) = f(a + (X-a))$ ausmultipliziert.) Leiten wir beide Seiten dieser Identität k Mal ab und setzen dann a für X ein, so fallen die meisten Terme weg; übrig bleibt nur noch

$$f^{(k)}(a) = b_k \cdot k!.$$

Stellt man diese Gleichung nach b_k um, folgt schon die Behauptung.