Musterlösung 26

Diskriminante, Zwischenkörper

1. Beweise die Formel für die Vandermonde-Determinante mit der Methode, mit der in der Vorlesung die Formel für die Resultante in Termen der Nullstellen der beteiligten Polynome bewiesen wurde.

   Erinnerung aus der Linearen Algebra: Sei R ein kommutativer Ring mit 1 und seien $a_1, \dots, a_n \in R$ beliebig. Dann hat die Matrix $A = (a_i^{j-1})_{1 \leqslant i,j \leqslant n}$ die *Vandermonde-Determinante* $\det(A) = \prod_{1 \leqslant i < j \leqslant n}(a_j - a_i)$.

   Lösung: Wenn die Formel für die Vandermonde-Determinante für unabhängige Variablen $X_1, \dots, X_n$ über $\mathbb{Z}$ stimmt, stimmt sie durch Einsetzen auch für beliebige Ringelemente $a_1, \dots, a_n$. Wir interessieren uns also für das Polynom

   $$V := \begin{vmatrix} 1 & X_1 & X_1^2 & \dots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \dots & X_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & X_n^2 & \dots & X_n^{n-1} \end{vmatrix} \in \mathbb{Z}[X_1, \dots, X_n].$$

   Betrachte beliebige Indizes $1 \leqslant i < j \leqslant n$. Wenn wir die Variable X_j gleich X_i setzen, wird die j-te Zeile der Matrix gleich der i-ten Zeile und folglich die Determinante zu null. Also hat V, als Polynom in X_j betrachtet, die Nullstelle X_i, und ist folglich durch $X_j - X_i$ teilbar. Da die Polynome $X_j - X_i$ für alle $1 \leqslant i < j \leqslant n$ paarweise teilerfremd sind, ist V somit auch schon durch $\prod_{i<j}(X_j - X_i)$ teilbar, das heisst, es gilt $V = c \cdot \prod_{i<j}(X_j - X_i)$ für ein Polynom $c \in \mathbb{Z}[X_1, \dots, X_n]$.

   Für jedes j ist die j-te Spalte der Matrix homogen vom Grad $j-1$, also ist V homogen vom Grad $\sum_{j=1}^{n}(j-1) = \frac{n(n-1)}{2}$. Dies ist aber auch schon der Grad von $\prod_{i<j}(X_j - X_i)$. Folglich muss c den Grad 0 haben; somit ist $c \in \mathbb{Z}$.

   In der Vorlesung haben wir c bestimmt, indem wir konkrete Werte eingesetzt haben, für die die Determinante einfach zu berechnen war. Im vorliegenden Fall scheint es keine geeigneten Werte zu geben, daher wählen wir eine andere Methode, nämlich Koeffizientenvergleich. Nach Definition ist

   $$V = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot X_{\sigma 2}^1 \cdots X_{\sigma n}^{n-1}.$$

   Also ist der Koeffizient von $X_2^1 \cdots X_n^{n-1}$ in V gleich $+1$. Wir behaupten das gleiche für das Polynom $\prod_{1 \leqslant i < j \leqslant n}(X_j - X_i)$. Beim Ausmultiplizieren entsteht nur dann

der Term X_n^{n-1}, wenn wir aus allen Faktoren der Form $(X_n - X_i)$ den Term X_n auswählen. Übrig bleibt dann das Produkt $\prod_{1 \leqslant i < j \leqslant n-1}(X_j - X_i)$, für welches wir genauso argumentieren können mit X_{n-1}^{n-2}, und so weiter. Insgesamt zeigt dies, dass beim Ausmultiplizieren nur dann das Monom $X_2^1 \cdots X_n^{n-1}$ entsteht, wenn wir aus jedem Faktor $X_j - X_i$ mit $i < j$ das X_j auswählen. Der Koeffizient von $X_2^1 \cdots X_n^{n-1}$ ist also ebenfalls gleich $+1$. Durch Koeffizientenvergleich folgt somit $c = 1$, und wir sind fertig.

2. Sei R ein Ring, und betrachte das Polynom $f(X) = X^m + aX + b \in R[X]$ mit $m \geqslant 2$. Verifiziere die folgende Formel für die Diskriminante von f:

$$\mathrm{Disc}_f = (-1)^{m(m-1)/2}[(1-m)^{m-1}a^m + m^m b^{m-1}].$$

Lösung: Da f normiert ist, gilt $\mathrm{Disc}_f = (-1)^{m(m-1)/2} \det(\mathrm{Sylv}_{f,f'})$, wobei $\mathrm{Sylv}_{f,f'}$ die Sylvestermatrix von f und seiner Ableitung f' bezeichnet. Wir berechnen dies mit $f(X) = X^m + aX + b$ und $f'(X) = mX^{m-1} + a$:

$$\mathrm{Sylv}_{f,f'} = \begin{pmatrix} 1 & 0 & \cdots & 0 & a & b & & 0 \\ & \ddots & \cdots & \cdots & \cdots & \ddots & \ddots & \\ 0 & & 1 & 0 & \cdots & 0 & a & b \\ m & \cdots & \cdots & 0 & a & & & 0 \\ & \ddots & & \cdots & \cdots & \ddots & & \\ 0 & & & m & \cdots & 0 & a & \\ & & & & m & \cdots & 0 & a \end{pmatrix}$$

Für jedes $1 \leqslant k \leqslant m-1$ subtrahieren wir das m-fache der k-ten Zeile von der $k+m-1$-ten Zeile. So erhalten wir eine obere Blockdreiecksmatrix mit einer $(m-1) \times (m-1)$-Einheitsmatrix in der oberen linken Ecke und der Nullmatrix unter ihr. Also können wir die ersten $m-1$ Spalten und Zeilen streichen und erhalten

$$\det(\mathrm{Sylv}_{f,f'}) = \det \begin{pmatrix} (1-m)a & -mb & & & & 0 \\ & \ddots & & \ddots & & \\ 0 & & & & (1-m)a & -mb \\ m & 0 & \cdots & \cdots & 0 & a \end{pmatrix}.$$

Durch Entwicklung dieser Determinante nach der letzten Zeile erhalten wir

$$\det(\mathrm{Sylv}_{f,f'}) = m(mb)^{m-1} + a((1-m)a)^{m-1}$$

und berechnen

$$\begin{aligned}\mathrm{Disc}_f &= (-1)^{m(m-1)/2}\det(\mathrm{Sylv}_{f,f'})\\ &= (-1)^{m(m-1)/2}[m(mb)^{m-1} + a((1-m)a)^{m-1}]\\ &= (-1)^{m(m-1)/2}[(1-m)^{m-1}a^m + m^m b^{m-1}].\end{aligned}$$

3. Bestimme für jedes der folgenden ganzzahligen Polynome f, ob es separabel in $\mathbb{Q}[X]$ ist, sowie für welche Primzahlen f mod (p) separabel in $\mathbb{F}_p[X]$ ist.

   (a) $f(X) = X^5 + 5X + 5$,

   (b) $f(X) = X^4 - 5X^3 + 6X^2 + 4X - 8$.

   (c) $f(X) = X^5 + 2X^3 + 4$,

   Wie geht es schneller: mit der Diskriminante oder durch Berechnung des grössten gemeinsamen Teilers des Polynoms f und seiner Ableitung f' ?

   Lösung: Nach §5.10 der Vorlesung ist ein Polynom f über einem Körper K separabel genau dann, wenn f und f' teilerfremd sind. Nach §6.4 der Vorlesung ist dies auch äquivalent dazu, dass die Diskriminante $\mathrm{Disc}_f \neq 0$ ist. Es genügt also, entweder $\mathrm{ggT}(f, f')$ oder Disc_f zu berechnen. Letzteres benötigt die Determinante der Sylvestermatrix $\mathrm{Sylv}_{f,f'}$. Für $n = \deg(f)$ ist dies eine $(2n-1) \times (2n-1)$-Matrix, deren Determinante im Allgemeinen relativ aufwendig zu berechnen ist. Die Methode mit dem ggT ist daher oft einfacher.

   (a) Nach Aufgabe 2 hat das Polynom $f(X) = X^5 + 5X + 5$ die Diskriminante

   $$\mathrm{Disc}_f \;=\; (-1)^{5(5-1)/2}[(1-5)^{5-1}5^5 + 5^5 5^{5-1}] \;=\; 4^4 \cdot 5^5 + 5^5 \cdot 5^4 \;=\; 5^5 \cdot 881 \;\neq\; 0.$$

   Folglich ist f separabel in $\mathbb{Q}[X]$. Da 5 und 881 Primzahlen sind, ist f mod (p) separabel in $\mathbb{F}_p[X]$ genau dann, wenn $p \neq 5, 881$ ist. (*Aliter:* Nach dem Eisensteinkriterium für $p = 5$ ist das Polynom irreduzibel in $\mathbb{Q}[X]$ und wegen $\mathrm{char}(\mathbb{Q}) = 0$ folglich separabel in $\mathbb{Q}[X]$.)

   (b) Wir berechnen $\mathrm{ggT}(f, f')$ in $\mathbb{Q}[X]$ mit dem euklidischen Algorithmus. Dass der ggT sich nicht ändert, wenn wir die Polynome mit Elementen von $\mathbb{Q}^\times$ multiplizieren, benutzen wir während der Rechnung dazu, dass die Koeffizienten ganzzahlig bleiben.

   $$\begin{aligned}\mathrm{ggT}(f, f') &= \mathrm{ggT}(X^4 - 5X^3 + 6X^2 + 4X - 8, 4X^3 - 15X^2 + 12X + 4)\\ &\sim \mathrm{ggT}(4X^3 - 15X^2 + 12X + 4, X^2 - 4X + 4)\\ &\sim \mathrm{ggT}(X^2 - 4X + 4, 0)\\ &\sim X^2 - 4X + 4 \;=\; (X-2)^2.\end{aligned}$$

   Folglich ist 2 eine doppelte Nullstelle von $\mathrm{ggT}(f, f')$ und damit eine dreifache Nullstelle von $f(X) = X^4 - 5X^3 + 6X^2 + 4X - 8$. Also ist f nicht separabel in $\mathbb{Q}[X]$, und a fortiori auch nicht in $\mathbb{F}_p[X]$.

(c) Wir berechnen den ggT von f und f' in $\mathbb{Q}[X]$ wiederum mit Hilfe des euklidischen Algorithmus.

$$\begin{aligned}\mathrm{ggT}(f, f') &= \mathrm{ggT}(X^5 + 2X^3 + 8, 5X^4 + 6X^2)\\ &\sim \mathrm{ggT}(5X^2 + 6, X^3 + 10)\\ &\sim \mathrm{ggT}(5X^2 + 6, 3X - 25)\\ &\sim \mathrm{ggT}(3X - 25, 225X + 18)\\ &\sim \mathrm{ggT}(3X - 25, 5679) \sim 1.\end{aligned}$$

Folglich sind f und f' teilerfremd und f ist separabel in $\mathbb{Q}[X]$.

Modulo p: In der obigen Rechnung wurde mit Produkten der Primzahlen 2, 3 und 5 erweitert. Diese Fälle müssen wir deshalb getrennt betrachten. Für alle übrigen Primzahlen gilt die obige Rechnung genauso modulo (p). Wegen $5679 = 3^2 \cdot 631$ mit 631 prim ist also f mod (p) separabel für alle $p \notin \{2, 3, 5, 631\}$ und inseparabel für $p = 631$.

Für $p = 2$ ist $f(X) \equiv X^5$ mod (2) mit der fünffachen Nullstelle 0; also ist f mod (2) inseparabel.

Für $p = 3$ ist $f'(X) = 5X^4 + 6X^2 \equiv 2X^4$ mod (3) mit der vierfachen Nullstelle 0, es gilt jedoch $f(0) = 4 \not\equiv 0$ mod (3). Somit ist f mod (3) separabel.

Für $p = 5$ gilt $f'(X) = 5X^4 + 6X^2 \equiv X^2$ mod (5) mit der zweifachen Nullstelle 0, es gilt jedoch $f(0) = 4 \not\equiv 0$ mod (5). Somit ist f mod (5) separabel.

Insgesamt ist also f mod (p) separabel genau dann, wenn $p \notin \{2, 631\}$ ist.

4. Sei $\underline{X} := (X_1, X_2, X_3, X_4)$ ein Satz unabhängiger Variablen über einem Körper K, und sei $\underline{S} := (S_1, S_2, S_3, S_4)$ mit den zugehörigen elementarsymmetrischen Polynomen.

   (a) Bestimme ein primitives Element der Erweiterung $K(\underline{X})/K(\underline{S})$.

   (b) Sei $\Delta := \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle \triangleleft S_4$ die Kleinsche Vierergruppe. Bestimme $K(\underline{X})^\Delta$ durch explizite Erzeugende über $K(\underline{S})$.

Lösung: (a) Das Element $X_1^3X_2^2X_3$ hat trivialen Stabilisator in S_4, ist also für kein $1 \lneq \Gamma \leqslant S_4$ in $K(\underline{X})^\Gamma$ enthalten. Das bedeutet, dass $\mathrm{Gal}(K(\underline{X})/K(\underline{S})(X_1^3X_2^2X_3))$ trivial ist, und mit dem Hauptsatz der Galoistheorie folgt $K(\underline{S})(X_1^3X_2^2X_3) = K(\underline{X})$.

(b) Sei T eine weitere unabhängige Variable. Nach dem Satz aus Abschnitt 6.5

wird $K(\underline{X})$ dann durch die Koeffizienten des Polynoms

$$\begin{aligned}
&\prod_{\delta\in\Delta}(T-\delta(X_1^3X_2^2X_3)) = (T - X_1^3X_2^2X_3)(T - X_2^3X_1^2X_4)(T - X_3^3X_4^2X_1)(T - X_4^3X_3^2X_2)\\
&\quad= T^4 - (X_1^3X_2^2X_3 + X_2^3X_1^2X_4 + X_3^3X_4^2X_1 + X_4^3X_3^2X_2)T^3\\
&\qquad + (X_1^3X_2^2X_3X_2^3X_1^2X_4 + X_1^3X_2^2X_3X_3^3X_4^2X_1 + X_1^3X_2^2X_3X_4^3X_3^2X_2\\
&\qquad + X_2^3X_1^2X_4X_3^3X_4^2X_1 + X_2^3X_1^2X_4X_4^3X_3^2X_2 + X_3^3X_4^2X_1X_4^3X_3^2X_2)T^2\\
&\qquad - (X_2^3X_1^2X_4X_3^3X_4^2X_1X_4^3X_3^2X_2 + X_1^3X_2^2X_3X_3^3X_4^2X_1X_4^3X_3^2X_2\\
&\qquad + X_1^3X_2^2X_3X_2^3X_1^2X_4X_4^3X_3^2X_2 + X_1^3X_2^2X_3X_2^3X_1^2X_4X_3^3X_4^2X_1)T\\
&\qquad + X_1^3X_2^2X_3X_2^3X_1^2X_4X_3^3X_4^2X_1X_4^3X_3^2X_2\\
&\quad= T^4 - (X_1^3X_2^2X_3 + X_1^2X_2^3X_4 + X_1X_3^3X_4^2 + X_2X_3^2X_4^3)T^3\\
&\qquad + X_1X_2X_3X_4(X_1^4X_2^4 + X_1^3X_2X_3^3X_4 + 2X_1^2X_2^2X_3^2X_4^2 + X_1X_2^3X_3X_4^3 + X_3^4X_4^4)T^2\\
&\qquad - (X_1X_2X_3X_4)^3(X_2X_3^2X_4^3 + X_1X_3^3X_4^2 + X_1^2X_2^3X_4 + X_1^3X_2^2X_3)T\\
&\qquad + X_1^6X_2^6X_3^6X_4^6
\end{aligned}$$

erzeugt. Durch Ignorieren von Termen in $K(\underline{S})$ erhalten wir die beiden Erzeuger

$$\begin{aligned}
&X_1^3X_2^2X_3 + X_1^2X_2^3X_4 + X_1X_3^3X_4^2 + X_2X_3^2X_4^3,\\
&X_1^4X_2^4 + X_1^3X_2X_3^3X_4 + X_1X_2^3X_3X_4^3 + X_3^4X_4^4.
\end{aligned}$$

Aliter: Wir probieren es mit der Summe aller Δ-Konjugierten des primitiven Elements aus (a), also mit

$$\sum_{\delta\in\Delta}\delta(X_1^3X_2^2X_3) \;=\; X_1^3X_2^2X_3 + X_1^2X_2^3X_4 + X_1X_3^3X_4^2 + X_2X_3^2X_4^3.$$

Wir rechnen explizit nach, dass sein Stabilisator in S_4 schon gleich Δ ist. Also liegt es in keinem kleineren Zwischenkörper, und es ist schon alleine ein Erzeugendes von $K(\underline{X})^\Delta$ über $K(\underline{S})$.

Aliter: Wir suchen Δ-invariante homogene Polynome von möglichst kleinem Grad. Alle solche vom Grad 0 oder 1 sind schon S_4-invariant, interessieren uns also nicht. In Grad 2 finden wir aber die $\Delta = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$-invarianten Polynome $X_1X_2 + X_3X_4$ und $X_1X_3 + X_2X_4$ und $X_1X_4 + X_2X_3$. Der Stabilisator von $X_1X_2 + X_3X_4$ in S_4 ist $\langle\Delta\cup\{(1\,2), (3\,4)\}\rangle$ (isomorph zu D_4), der Stabilisator von $X_1X_3 + X_2X_4$ ist $\langle\Delta\cup\{(1\,3), (2\,4)\}\rangle$. Der Schnitt dieser beiden Stabilisatoren ist genau Δ, deshalb sind die Polynome $X_1X_2 + X_3X_4$ und $X_1X_3 + X_2X_4$ Erzeuger von $K(\underline{X})^\Delta$ über $K(\underline{S})$ (und $X_1X_4 + X_2X_3$ ist als Bonus mit dabei).

5. Sei $n \geqslant 3$ und sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Zeige, dass $\mathbb{Q}(\zeta)\cap\mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$ ist.

   Lösung: Sei $K := \mathbb{Q}(\zeta)\cap\mathbb{R}$. Da ζ^{-1} zu ζ komplex konjugiert ist, gilt $\zeta + \zeta^{-1} \in \mathbb{R}$, also ist $\mathbb{Q}(\zeta+\zeta^{-1}) \subset K$. Wegen $\zeta \notin \mathbb{R}$ ist weiter $K \subsetneq \mathbb{Q}(\zeta)$, also folgt $[\mathbb{Q}(\zeta)/K] \geqslant 2$. Andererseits ist ζ eine Nullstelle des Polynoms $X^2-(\zeta+\zeta^{-1})X+1 \in \mathbb{Q}(\zeta+\zeta^{-1})[X]$, folglich gilt $[\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})] = 2$ und somit ist $\mathbb{Q}(\zeta + \zeta^{-1}) = K$.