WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

25. November 2020

9. Übungsblatt Algebra

Aufgabe 1: *(9 Punkte)*

a) Zeigen Sie, daß $\mathbb{Q}(\sqrt{28},\sqrt{35})$, $\mathbb{Q}(\sqrt{5},\sqrt{7})$ und $\mathbb{Q}(\sqrt{7}-\sqrt{5})$ denselben Teilkörper K von $\mathbb{R}$ definieren!

Lösung: Da $\sqrt{28}=2\sqrt{7}$ und $\sqrt{35}=\sqrt{5}\sqrt{7}$, liegen $\sqrt{28}$ und $\sqrt{35}$ in $\mathbb{Q}(\sqrt{5},\sqrt{7})$; genauso liegt auch $\sqrt{7}=\frac{1}{2}\sqrt{28}$ in $\mathbb{Q}(\sqrt{28},\sqrt{35})$, und damit auch der Quotient $\sqrt{35}/\sqrt{7}=\sqrt{5}$. Somit ist $\mathbb{Q}(\sqrt{5},\sqrt{7})=\mathbb{Q}(\sqrt{28},\sqrt{35})$.
$k=\mathbb{Q}(\sqrt{7}-\sqrt{5})$ liegt natürlich in $\mathbb{Q}(\sqrt{3},\sqrt{7})$. Als Körper enthält k auch das Quadrat $(\sqrt{7}-\sqrt{5})^2=12-2\sqrt{35}$, also auch $\sqrt{35}$ und $\sqrt{35}(\sqrt{7}-\sqrt{5})=(7\sqrt{5}-5\sqrt{7})$. Damit liegt auch $(7\sqrt{5}-5\sqrt{7})+5(\sqrt{7}-\sqrt{5})=6\sqrt{5}$ in k, also auch $\sqrt{5}$ und $\sqrt{7}=(\sqrt{7}-\sqrt{5})+\sqrt{5}$. Also ist $k=\mathbb{Q}(\sqrt{5},\sqrt{7})$.

b) Welchen Grad hat die Körpererweiterung $K/\mathbb{Q}$? Geben Sie eine möglichst einfache Basis von $K/\mathbb{Q}$ an!

Lösung: $K=\mathbb{Q}(\sqrt{3},\sqrt{7})$ enthält den Körper $\mathbb{Q}(\sqrt{3})$; als Vektorraum über $\mathbb{Q}(\sqrt{3})$ ist $K=\mathbb{Q}(\sqrt{3})\oplus\mathbb{Q}(\sqrt{3})\sqrt{7}$. Da $\mathbb{Q}(\sqrt{3})=\mathbb{Q}\oplus\mathbb{Q}\sqrt{3}$ ist, folgt $K=\mathbb{Q}\oplus\mathbb{Q}\sqrt{3}\oplus\mathbb{Q}\sqrt{7}\oplus\mathbb{Q}\sqrt{21}$. Damit ist $[K:\mathbb{Q}]=4$.

c) Zeigen Sie, daß $K/\mathbb{Q}$ GALOISsch ist, und bestimmen Sie $\mathrm{Aut}(K/\mathbb{Q})$!

Lösung: Ein Automorphismus $\varphi\in\mathrm{Aut}(K/\mathbb{Q})$ muß $\mathbb{Q}$ festlassen, ist also eindeutig bestimmt durch die Bilder der Basiselemente. Natürlich muß $\varphi(1)=1$ sein. Da $\left(\sqrt{3}\right)^2=3$ ist, muß auch $\varphi\left(\sqrt{3}\right)^2=\varphi(3)=3$ sein, d.h. $\varphi\left(\sqrt{3}\right)=\pm\sqrt{3}$. Ein analoges Argument zeigt, daß $\varphi\left(\sqrt{7}\right)=\pm\sqrt{7}$ sein muß. Das noch fehlende Bild $\varphi\left(\sqrt{21}\right)=\varphi\left(\sqrt{3}\right)\cdot\varphi\left(\sqrt{7}\right)$ ist durch die Bilder von $\sqrt{3}$ und $\sqrt{7}$ festgelegt. Also haben wir vier Automorphismen; abgesehen von der Identität sind dies die Abbildungen ρ,σ,τ mit $\rho\left(\sqrt{3}\right)=-\sqrt{3}$ und $\rho\left(\sqrt{7}\right)=\sqrt{7}$, $\sigma\left(\sqrt{3}\right)=\sqrt{3}$ und $\sigma\left(\sqrt{7}\right)=-\sqrt{7}$, $\tau\left(\sqrt{3}\right)=-\sqrt{3}$ und $\tau\left(\sqrt{7}\right)=-\sqrt{7}$.

d) Bestimmen Sie alle Körper L mit $\mathbb{Q}<L<K$!

Lösung: Die Erweiterung $K/\mathbb{Q}$ ist GALOISsch, denn ist $x=a+b\sqrt{3}+c\sqrt{7}+d\sqrt{21}$ ein Element des Fixkörpers von $\mathrm{Aut}(K/\mathbb{Q})$, ist $\rho(x)=a-b\sqrt{3}+c\sqrt{7}-d\sqrt{21}=x$, also ist wegen der Eindeutigkeit der Basisdarstellung $b=d=0$. Genauso folgt aus $\sigma(x)=x$, daß $c=0$ sein muß. Daher ist $x=a\in\mathbb{Q}$, der Fixkörper ist also $\mathbb{Q}$.
Die GALOIS-Gruppe hat vier Elemente; außer der Identität erzeugt jedes eine Untergruppe der Ordnung zwei. Die Zwischenkörper sind daher

$$K^{<\rho>}=\mathbb{Q}(\sqrt{7}),\qquad K^{<\sigma>}=\mathbb{Q}(\sqrt{3})\quad\text{und}\quad K^{<\tau>}=\mathbb{Q}(\sqrt{21})\,,$$

wobei $<g>$ jeweils die von einem Element g erzeugte zyklische Untergruppe bezeichnet.

e) Finden Sie ein irreduzibles Polynom f derart, daß $K \cong \mathbb{Q}[X]/(f)$ ist!

Lösung: Wir wissen aus *a)*, daß $\left(\sqrt{7}-\sqrt{3}\right)^2 = 10 - 2\sqrt{21}$ ist. Für $x = \sqrt{7}-\sqrt{3}$ ist also $(x^2-10)^2 = 4\cdot 21 = 84$, d.h. $f = X^4 - 20X^2 + 16$ hat $\sqrt{7}-\sqrt{3}$ als Nullstelle. Da f rationale Koeffizienten hat, muß f auch die Bilder von $\sqrt{7}-\sqrt{3}$ unter den Automorphismen von $K/\mathbb{Q}$ als Nullstellen haben, d.h. f verschwindet für jede der vier Zahlen $\pm\sqrt{7}\pm\sqrt{3}$. Wäre f nicht irreduzibel in $\mathbb{Q}[X]$, gäbe es ein Polynom $g \in \mathbb{Q}[X]$ vom Grad kleiner vier, das an der Stelle $\sqrt{7}-\sqrt{3}$ verschwindet, und auch g müßte alle vier Bilder als Nullstellen haben. Dies ist für ein Polynom vom Grad kleiner vier nicht möglich; somit ist f irreduzibel. Da $\mathbb{Q}(x)/\mathbb{Q}$ eine Erweiterung vom Grad vier ist, folgt $K \cong \mathbb{Q}[X]/(f)$.

f) Zerlegen Sie f über dem Körper $\mathbb{Q}\left(\sqrt{7}\right)$ in seine irreduziblen Faktoren!

Lösung: $\mathbb{Q}\left(\sqrt{7}\right)$ ist der Fixkörper von ρ; ein Faktor, der $\sqrt{7}-\sqrt{3}$ als Nullstelle hat, muß daher auch $\rho\left(\sqrt{7}-\sqrt{3}\right) = \sqrt{7}+\sqrt{3}$ als Nullstelle haben.

$$g = \left(X-\sqrt{7}+\sqrt{3}\right)\left(X-\sqrt{7}-\sqrt{3}\right) = \left(X-\sqrt{7}\right)^2 - 3 = X^2 - 2\sqrt{7} + 4$$

ist ein Polynom aus $\mathbb{Q}\left(\sqrt{7}\right)[X]$ mit diesen beiden Nullstellen. Das Polynom

$$h = \left(X+\sqrt{7}+\sqrt{3}\right)\left(X+\sqrt{7}-\sqrt{3}\right) = \left(X+\sqrt{7}\right)^2 - 3 = X^2 + 2\sqrt{7} + 4$$

liegt ebenfalls dort und verschwindet bei den beiden übrigen Nullstellen von f. Somit ist

$$f = \left(X+\sqrt{3}+\sqrt{7}\right)\left(X-\sqrt{3}+\sqrt{7}\right)\left(X+\sqrt{3}-\sqrt{7}\right)\left(X-\sqrt{3}-\sqrt{7}\right) = gh\,,$$

und g, h sind irreduzibel über $\mathbb{Q}\left(\sqrt{7}\right)$, da jedes Polynom über diesem Körper mit einem Element aus K auch dessen Bild unter ρ als Nullstelle haben muß.

Aufgabe 2: *(4 Punkte)*
G sei eine Gruppe, und $\chi_1, \ldots, \chi_r$ seien paarweise verschiedene Gruppenhomomorphismen von G in die multiplikative Gruppe $\mathbb{Q}^\times$. Zeigen Sie, daß die χ_i linear unabhängig sind, d.h. falls $a_1\chi_1(x) + \cdots + a_r\chi_r(x) = 0$ für alle $x \in G$ und irgendwelche $a_i \in \mathbb{Q}$, müssen alle a_i verschwinden. *(Hinweis: Benutzen Sie die Methode, mit der in der Vorlesung die „lineare Unabhängigkeit" für Monomorphismen von Körpern bewiesen wurde!)*

Lösung: Beweis durch Induktion nach r. Der Fall $r = 1$ ist trivial; sei also $r > 1$, und die Behauptung sei bewiesen für alle Summen mit weniger als r Summanden. Ist

$$a_1\chi_1(x) + a_2\chi_2(x) \cdots + a_r\chi_r(x) = 0$$

für alle $x \in G$, so ist auch

$$\begin{aligned} &a_1\chi_1(xy) + a_2\chi_2(xy) + \cdots + a_r\chi_r(xy) \\ &= a_1\chi_1(y)\chi_1(x) + a_2\chi_2(y)\chi_2(x) + \cdots + a_r\chi_r(y)\chi_r(x) = 0 \end{aligned}$$

für alle $x, y \in G$. Multiplikation der ursprünglichen Gleichung mit $\chi_1(y)$ zeigt, daß auch

$$a_1\chi_1(y)\chi_1(x) + a_2\chi_1(y)\chi_2(x) + \cdots + a_r\chi_1(y)\chi_r(x) = 0$$

ist. Die Differenz der beiden letzten Gleichungen ist

$$a_2\left(\chi_2(y) - \chi_1(y)\right) + \cdots + a_r\left(\chi_r(y) - \chi_1(y)\right) = 0\,.$$

Nach Induktionsannahme müssen daher alle Koeffizienten $a_i\left(\chi_i(y) - \chi_1(y)\right)$ verschwinden. Falls wir y so wählen, daß $\chi_r(y) \neq \chi_1(y)$ ist, folgt, daß auch der Koeffizient a_r verschwinden muß. Damit hat die ursprüngliche Relation höchstens $r-1$ Summanden; nach Induktionsvoraussetzung müssen daher alle Koeffizienten a_i verschwinden.

Aufgabe 3: *(7 Punkte)*

a) Zeigen Sie: Eine Untergruppe $U < \mathfrak{S}_n$ der symmetrischen Gruppe $\mathfrak{S}_n$ ist genau dann ein Normalteiler, wenn für jede Transposition $(a\ b) \in \mathfrak{S}_n$ und jede Permutation $\pi \in U$ gilt: $(a\ b)\pi(a\ b) \in U$.

Lösung: U ist genau dann ein Normalteiler, wenn für jedes $\pi \in U$ und jede Permutation $\omega \in \mathfrak{S}_n$ auch $\omega^{-1}\pi\omega$ in U liegt. Falls U ein Normalteiler ist, muß also insbesondere für jede Transposition $(a\ b)$ gelten, daß $(a\ b)^{-1}\pi(a\ b) = (a\ b)\pi(a\ b)$ in U liegt.
Umgekehrt gelte dies für alle $\pi \in U$ und alle Transpositionen $(a\ b)$. Jede Permutation $\omega \in \mathfrak{S}_n$ läßt sich schreiben als Produkt $\omega = (a_1\ b_1)\cdots(a_r\ b_r)$ von Transpositionen. Da jede Transposition zu sich selbst invers ist, ist dann $\omega^{-1} = (a_r\ b_r)\cdots(a_1\ b_1)$ und

$$\omega^{-1}\pi\omega = (a_r\ b_r)\cdots(a_1\ b_1)\pi(a_1\ b_1)\cdots(a_r\ b_r)\,.$$

Nach Voraussetzung liegt $\pi_{r-1} \underset{\text{def}}{=} (a_r\ b_r)\pi(a_r\ b_r)$ in U, genauso auch das Element $\pi_{r-2} \underset{\text{def}}{=} (a_{r-1}\ b_{r-1})\pi_{r-1}(a_{r-1}\ b_{r-1})$, und so weiter. Also liegt $\omega^{-1}\pi\omega$ in U, und U ist Normalteiler.

b) $U \leq \mathfrak{S}_4$ sei die von den beiden Permutationen $(1\ 2)(3\ 4)$ und $(1\ 3)(2\ 4)$ erzeugte Untergruppe. Wie viele Elemente hat U?

Lösung: Da elementfremde Zykeln kommutieren, haben beide Erzeugende die Ordnung zwei. $(1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3)$, und auch $(1\ 3)(2\ 4)(1\ 2)(3\ 4) = (1\ 4)(2\ 3)$. Die Ordnung dieses Elements ist ebenfalls zwei. Somit besteht U aus vier Elementen: Der Identität, den beiden Erzeugenden und deren Produkt.

c) Ist U zyklisch?

Lösung: Nein; da alle Elemente die Ordnung zwei haben, kann es kein Element der Ordnung vier geben.

d) Zeigen Sie, daß U ein Normalteiler von $\mathfrak{S}_4$ ist!
Hinweis: Betrachten Sie alle Produkte $(e\ f)(a\ b)(c\ d)(e\ f)$ mit $\{a,b,c,d\} = \{1,2,3,4\}$ und $\{e,f\} \subset \{1,2,3,4\}$, und überlegen Sie sich, daß das Ergebnis in erster Linie davon abhängt, wie viele Elemente $\{a,b\} \cap \{e,f\}$ hat.

Lösung: Wie wir gerade gesehen haben, besteht U abgesehen von der Identität genau aus den Elementen $(a\ b)(c\ d)$ mit $\{a,b,c,d\} = \{1,2,3,4\}$. Um zu sehen, daß U ein Normalteiler ist, reicht es nach *a)* zu zeigen, daß für jede Transposition $(e\ f)$ auch $(e\ f)(a\ b)(c\ d)(e\ f)$ in U liegt. Der Durchschnitt der Mengen $\{e,f\}$ und $\{a,b\}$ kann leer sein oder ein- oder zweielementig. $\{e,f\} \cap \{a,b\} = \emptyset$ ist gleichbedeutend mit $\{e,f\} = \{c,d\}$ und $(e\ f) = (c\ d)$. Dann ist

$$(e\ f)(a\ b)(c\ d)(e\ f) = (c\ d)(a\ b)(c\ d)(c\ d) = (c\ d)(a\ b) = (a\ b)(c\ d) \in U\,.$$

Bei einem einelementigen Durchschnitt können wir o.B.d.A. annehmen, daß dieser aus a besteht; dann ist $a = e$ und wieder ohne Beschränkung der Allgemeinheit können wir annehmen, daß $f = c$ ist. Also ist

$$(e\ f)(a\ b)(c\ d)(e\ f) = (a\ c)(a\ b)(c\ d)(a\ c) = (a\ d)(b\ c) \in U\,.$$

Hat der Durchschnitt zwei Elemente, ist $\{a,b\} = \{e,f\}$ und $(a\ b) = (e\ f)$, also

$$(e\ f)(a\ b)(c\ d)(e\ f) = (a\ b)(a\ b)(c\ d)(a\ b) = (c\ d)(a\ b) = (a\ b)(c\ d) \in U\,.$$

Damit ist die Bedingung in allen Fällen erfüllt, d.h. U ist Normalteiler.

e) Folgern Sie, daß $\mathfrak{S}_4$ eine auflösbare Gruppe ist!

Lösung: $\mathfrak{A}_4$ ist als Kern der Signatur (oder als Untergruppe vom Index zwei) ein Normalteiler, und $\mathfrak{S}_4/\mathfrak{A}_4 \cong \mathbb{Z}/2$ ist zyklisch. U ist eine Untergruppe von $\mathfrak{A}_4$, denn alle vier Elemente von U sind gerade Permutationen. Als Normalteiler von $\mathfrak{S}_4$ ist U natürlich erst recht Normalteiler von $\mathfrak{A}_4$. Die alternierende Gruppe hat $4!/2 = 12$ Elemente; daher hat die Faktorgruppe $\mathfrak{A}_4/U$ drei Elemente und ist somit isomorph zu $\mathbb{Z}/3$. U ist nicht zyklisch, aber abelsch, so daß jede Untergruppe Normalteiler ist. Beispielsweise ist also die Untergruppe bestehend aus $(1\ 2)(3\ 4)$ und der Identität ein Normalteiler $N \cong \mathbb{Z}/2$ von U, und auch $U/N \cong \mathbb{Z}/2$. In der Reihe

$$\{\mathrm{id}\} < N < U < \mathfrak{A}_4 < \mathfrak{S}_4$$

ist also jede Gruppe Normalteiler der nächsten, und in allen Fällen ist die Faktorgruppe zyklisch. Somit ist $\mathfrak{S}_4$ auflösbar.