1.1 $n \in \mathbb{N}$, $n > 3$. σ Drehung $\mathbb{R}^2$ um $\phi = \frac{2\pi}{n}$. τ Spiegelung an y-Achse. $D_n = \langle \sigma, \tau \rangle$

Im folgenden wird $x \in \mathbb{R}^2$ angenommen.

(a) Es gilt $\operatorname{ord}(\sigma) = n$, $\operatorname{ord}(\tau) = 2$ und $\sigma\tau\sigma = \tau$.

$\operatorname{ord}(\sigma) = n$, da:

$$\sigma^i(x) = \begin{pmatrix} \cos(i \cdot \phi) & \sin(i \cdot \phi) \\ -\sin(i \cdot \phi) & \cos(i \cdot \phi) \end{pmatrix} \cdot x$$

Und damit:

$$\sigma^n(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot x = x \quad \sigma^n = \mathrm{id}$$

Für τ:

$$\tau(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot x \quad \tau^2(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot x = x \quad \tau^2 = \mathrm{id}$$

Damit ist $\operatorname{ord}(\tau) = 2$.

$$\sigma\tau\sigma(x) = \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} \cdot x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot x = \tau(x)$$

Es gilt also auch $\sigma\tau\sigma = \tau$

(b) Es gilt $D_n = \left\{ \tau^i \sigma^j \middle| i \in \{0,1\}, j \in \{0,1,\dots,n-1\} \right\}$.

D_n ist definiert als die kleinste Menge die τ und σ enthält und abgeschlossen ist unter Verknüpfung. Zunächst gilt:

$$M_n := \left\{ \tau^i \sigma^j \middle| i \in \{0,1\}, j \in \{0,1,\dots,n-1\} \right\} \subset D_n$$

Dies ist wahr, da $\tau \in D_n \to \tau^i \in D_n \; \forall i \in \mathbb{N}$, sowie analog $\sigma^j \in D_n \; \forall j \in \mathbb{N}$ implizieren (jeweils über die Abgeschlossenheit unter Verknüpfung), dass $\tau^i \sigma^j \in D_n \; \forall i, j \in \mathbb{N}$. Damit gilt $M_n \subset D_n$, da alle Elemente aus M_n in D_n enthalten sind.
Fehlt zu zeigen, dass M_n abgeschlossen ist unter Verknüpfung, sowie dass σ und τ in M_n sind. Für letzteres reicht j und i als 1 beziehungsweise 0 zu wählen. M_n ist abgeschlossen unter Verknüpfung, da:

$$\tau^i \sigma^j \tau^k \sigma^l$$

Für $k, i \in \{0,1\}$ und $j, l \in \{0,\dots,n-1\}$ Fälle:

$k = 0$ In diesem Fall ist:

$$\tau^i \sigma^j \tau^k \sigma^l = \tau^i \sigma^{j+l} = \tau^i \sigma^{j+l \mod n} \in M_n$$

$k = 1$ In diesem Fall ist:

$$\begin{aligned} \tau^i \sigma^j \tau^k \sigma^l &= \tau^i \sigma^j \tau \sigma^l \\ &= \tau^i \sigma^{j-1} \sigma\tau\sigma \sigma^{l-1} \\ &= \tau^i \sigma^{j-1} \tau \sigma^{l-1} \\ &= \dots \\ &= \tau^{i+1} \sigma^{l-j} = \tau^{i+1 \mod 2} \sigma^{l-j \mod n} \in M_n \end{aligned}$$

Wobei jeweils $\sigma\tau\sigma = \tau$ und die Ordnungen von σ und τ ausgenutzt worden sind.

(c) D_n hat $2n$ Elemente und ist nicht kommutativ.

D_n ist nicht kommutativ, da $\tau\sigma\tau = \mathrm{id} \neq \tau\tau\sigma$. D_n hat $2n$ Elemente, da einerseits 2 und n die Gruppenordnung teilen müssen, und andererseits mehr als n Elemente enthalten sein können ($\langle\sigma\rangle \subset D_n$) und weniger als $2n$. Damit bleibt nur $2n$ als Anzahl der Elemente über.

1.2 K Körper und $f(x) \in K[x]$ irreduzibel, normiert. a Nullstelle von $f(x)$ in Erweiterungskörper von K.

(a) Beweisen Sie: Ist auch $f(a+1) = 0$, so gilt $\operatorname{char}(K) > 0$.

$f(a) = f(a+1) = 0$. Dann teilt $(x-a)(x-a-1)\ f$.
Ist $\operatorname{char}(K) = 0$, so ist K vollkommen. $f'(x) = (x-a-1)g(x) + (x-a)g(x) + ()$
Gelte nun weiter $\operatorname{char}(K) = p$ und $a^p - a \in K$.

(b) Beweisen Sie, dass $f(x) = x^p - x - (a^p - a)$ gilt.

$x^p - x - (a^p - a)$ besitzt die Nullstellen a und $a+1$, und ist irreduzibel, da $a \notin K$, normiert sowieso:

$$a^p - a - (a^p - a) = 0$$
$$(a+1)^p - (a+1) - (a^p - a) = (a+1)^p - a^p - 1 = (a^p + 1) - a^p - 1 = 0$$

Damit erfüllt $x^p - x - (a^p - a)$ die Definition von f. Es wurde ausgenutzt, dass $p|\binom{p}{i} \quad \forall\, p > i > 1$.

(c) Beweisen Sie, dass die Erweiterung $K(a)/K$ galoissch ist.

$f(x)$ ist das Minimalpolynom von a über K, also ist nach Satz 1.x die Körpererweiterung normal. Da nur ein Element adjungiert wird, ist die Körpererweiterung auch endlich. Da f separabel ist, ist die Körpererweiterung auch separabel und nach Satz 1.x galoissch

(d) Beweisen Sie, dass $\operatorname{Aut}(K(a);K)$ zyklisch von Ordnung p ist.

$\operatorname{Aut}(K(a);K)$ ist zyklisch von Ordnung p, da es p Nullstellen gibt, und es keine Zwischenkörper gibt (Galoiskorrespondenz)

1.3 $\mathbb{C}(x)$ rationale Funktionen über $\mathbb{C}$. In $\operatorname{Aut}(\mathbb{C}(x);\mathbb{C})$, betrachte σ, τ mit $\sigma(x) = -x$ und $\tau(x) = \mathrm{i}x^{-1}$. $G = \langle\sigma,\tau\rangle \subset \operatorname{Aut}(\mathbb{C}(x);\mathbb{C})$.

(a) Beweisen Sie, dass G endlich ist. Welche Ihnen bekannte Gruppe ist G?

Die Erzeuger σ und τ kommutieren

$$\sigma(\tau(x)) = \mathrm{i}(-x)^{-1} = -\mathrm{i}x^{-1} = \tau(\sigma(x))$$

und haben beide Ordnung 2:

$$\sigma^2(x) = -(-x) = x \quad \tau^2(x) = \mathrm{i}\left(\mathrm{i}x^{-1}\right)^{-1} = \mathrm{i} \cdot -\mathrm{i}x = x$$

Damit ist die Gruppe endlich.
Die Gruppe ist isomorph zur kleinschen Vierergruppe ($Z_2 \times Z_2$)

$$G = \left(-x, -\mathrm{i}x^{-1}, \mathrm{i}x^{-1}, \mathrm{id}\right)$$

Beweis durch Multiplikationstabelle:

	$-x$	$-\mathrm{i}x^{-1}$	$\mathrm{i}x^{-1}$	id
$-x$	id	$\mathrm{i}x^{-1}$	$-\mathrm{i}x^{-1}$	$-x$
$-\mathrm{i}x^{-1}$	$\mathrm{i}x^{-1}$	id	$-x$	$-\mathrm{i}x^{-1}$
$\mathrm{i}x^{-1}$	$-\mathrm{i}x^{-1}$	$-x$	id	$\mathrm{i}x^{-1}$
id	$-x$	$-\mathrm{i}x^{-1}$	$\mathrm{i}x^{-1}$	id

(b) Beweisen Sie, dass $\mathrm{Fix}\left(\mathbb{C}\left(x\right); G\right)$ rationaler Fkt-Körper über $\mathbb{C}$; $\mathrm{Fix}\left(\mathbb{C}\left(x\right); G\right) = \mathbb{C}\left(y\right)$ mit $y \in \mathbb{C}\left(x\right)$. y angeben.

Folgende Bedingungen müssen erfüllt sein:

$$y\left(x\right) = y\left(-x\right) \quad y\left(x\right) = y\left(\mathrm{i}x^{-1}\right)$$

$y\left(x\right) := x^2 - x^{-2}$ erfüllt beide Bedingungen. Nun muss gezeigt werden, dass beide Körper übereinstimmen. $\mathbb{C}\left(y\right) \subset \mathrm{Fix}\left(\mathbb{C}\left(x\right); G\right)$, da beide Bedingungen erfüllt sind. Die andere Inklusion folgt daraus, dass $y\left(x\right)$ minimalen Grad hat.