Aufgabe 1 (F06T1A2)**.** Sei $f = X^{17} + Y^{41}(X^3 + X + 1) - Y \in \mathbb{C}[X, Y]$.

(a) Man zeige, daß f als Polynom in X über dem Koeffizientenring $\mathbb{C}[Y]$ irreduzibel ist. (Hinweis: Eisenstein-Kriterium)

(b) Man zeige, daß f ein irreduzibles Element im Ring $\mathbb{C}[X, Y]$ ist.

(8 Punkte)

Lösung. (a) Wir stellen das Polynom f um, um zu verdeutlichen, daß wir es als Polynom in X mit Koeffizienten in $\mathbb{C}[Y]$ betrachten:

$$f = X^{17} + Y^{41}X^3 + Y^{41}X + (Y^{41} - Y).$$

Da $\mathbb{C}$ ein Körper ist, ist der Polynomring in einer Variablen $\mathbb{C}[Y]$ ein euklidischer Ring bezüglich der Gradabbildung und damit insbesondere faktoriell. In $\mathbb{C}[Y]$ ist Y ein irreduzibles Element, und da $\mathbb{C}[Y]$ faktoriell ist, ist es ein Primelement. Man sieht sofort, daß Y alle Koeffizienten bis auf den höchsten (der 1 ist) teilt, und daß Y^2 den konstanten Koeffizienten nicht teilt. Also erfüllt f die Voraussetzungen für das Eisenstein-Kriterium, und es folgt, daß f in $\mathbb{C}[Y][X]$ irreduzibel ist (und da f faktoriell ist, ist es sogar irreduzibel in $\mathbb{C}(Y)[X]$).

(b) Wir zeigen, daß $\mathbb{C}[Y][X] \cong \mathbb{C}[X, Y]$. Die Polynomringe $\mathbb{C}[Y]$ und $\mathbb{C}[X, Y]$ sind $\mathbb{C}$-Algebren. Nach der universellen Eigenschaft von Polynomalgebren gibt es genau einen $\mathbb{C}$-Algebrenhomomorphismus

$$\rho_1 : \mathbb{C}[Y] \to \mathbb{C}[X, Y]$$

mit $\rho_1(Y) = Y$. Es ist klar, daß er injektiv ist.
Wir fassen $\mathbb{C}[Y]$ vermittels ρ als Unterring von $\mathbb{C}[X, Y]$ auf. Damit ist $\mathbb{C}[X, Y]$, welches kommutativ ist, eine $\mathbb{C}[Y]$-Algebra. Nach der universellen Eigenschaft von Polynomalgebren, gibt es genau einen $\mathbb{C}[Y]$-Algebrenhomomorphismus,

$$\rho_2 : \mathbb{C}[Y][X] \to \mathbb{C}[X, Y]$$

mit $\rho_2(X) = X$. Dies ist insbesondere ein $\mathbb{C}$-Algebrenhomomorphismus, und es gilt, daß $\rho_2(Y) = Y$.
Andererseits gibt es nach der universellen Eigenschaft von Polynomalgebren genau einen $\mathbb{C}$-Algebrenhomomorphismus

$$\rho_3 : \mathbb{C}[X, Y] \to \mathbb{C}[Y][X]$$

mit $\rho_3(X) = X$ und $\rho_3(Y) = Y$. Man sieht sofort, daß ρ_2 und ρ_3 als $\mathbb{C}$-Algebrenhomomorphismen zueinander invers sind. Dies zeigt die Behauptung $\mathbb{C}[Y][X] \cong \mathbb{C}[X, Y]$.
Wir haben bereits gesehen, daß f irreduzibel in $\mathbb{C}[Y][X]$ ist. Via dem Isomorphismus ρ_3 folgt dann automatisch, daß f bereits irreduzibel in $\mathbb{C}[X, Y]$ ist.

Aufgabe 2 (H10T1A2)**.** Sei G eine Gruppe mit $|G| = 595 = 5 \cdot 7 \cdot 17$ und $H \leqslant G$ eine Untergruppe mit $|H| = 5$. Zeigen Sie:

(a) H ist ein Normalteiler von G.

(b) H liegt im Zentrum von G.

(6 Punkte)

Lösung. (a) Da die Primzahl 5 in der Gruppenordnung $|G| = 595 = 5 \cdot 7 \cdot 17$ in einfacher Potenz vorkommt, ist H eine 5-Sylow-Untergruppe von G. Eine Folgerung der Sätze von Sylow ist, daß eine p-Sylow-Untergruppe genau dann Normalteiler ist, wenn sie die einzige ist. Wir berechnen also die Anzahl s_5 der 5-Sylow-Untergruppen. Nach den Sätzen von Sylow gilt dafür

$$s_5 \Big| \frac{595}{5} = 7 \cdot 17 = 119 \qquad \text{und} \qquad s_5 \equiv 1 \mod 5.$$

Aus der ersten Aussage folgt $s_5 \in \{1, 7, 17, 119\}$. Da $7 \equiv 17 \equiv 2 \mod 5$, und somit $7 \cdot 17 \equiv 4 \mod 5$, muß also $s_5 = 1$ sein. Also ist H die einzige 5-Sylowuntergruppe von G und damit Normalteiler von G.

(b) Das Zentrum von G ist definiert als

$$Z(G) = \left\{ g \in G \;\middle|\; gxg^{-1} = x \forall x \in G \right\}.$$

Um zu zeigen, daß $H \subset Z(G)$. müssen wir also zeigen, daß für alle $h \in H$ und $g \in G$ gilt $ghg^{-1} = h$. Betrachte dazu die Abbildung

$$\kappa : G \to \mathrm{Aut}(H), g \mapsto \kappa_g\big|_H,$$

wobei $\kappa_g : G \to G, h \mapsto ghg^{-1}$ die Konjugation mit g ist. Da H Normalteiler ist, das heißt insbesondere für jedes $g \in G$ gilt $gHg^{-1} = H$, ist $\kappa_g\big|_H \in \mathrm{Aut}(H)$, also die Abbildung κ wohldefiniert. Der Kern $\ker(\kappa)$ ist ein Normalteiler von G. Nach dem Homomorphiesatz induziert κ einen injektiven Gruppenhomomorphismus

$$\widetilde{\kappa} : G/\ker(\kappa) \to \mathrm{Aut}(H).$$

Da H von Primzahlordnung ist, ist es zyklisch, genauer isomorph zu $\mathbb{Z}/(5)$, und seine Automorphismengruppe ist zyklisch von der Ordnung 4. Da $\widetilde{\kappa}$ injektiv ist, gilt

$$[G : \ker(\kappa)] \big| |\mathrm{Aut}(H)| = 4.$$

Andererseits gilt nach Lagrange, daß $[G : \ker(\kappa)] \big| |G| = 5 \cdot 7 \cdot 17$. Es folgt, daß $[G : \ker(\kappa)] = 1$, also $\ker(\kappa) = G$, und damit liegt H im Zentrum von G.

Aufgabe 3 (F06T3A6)**.** Sind L/K und M/L endliche Körpererweiterungen und ist M/K galoissch mit Galoisgruppe G, so ist auch der Körper

$$K(\bigcup_{\sigma \in G} \sigma(L))$$

galoissch über K. (5 Punkte)

Lösung. Für alle $\sigma \in G$ gilt $\sigma(L) \subset M$, also ist auch das Kompositum $\prod_{\sigma \in G} \sigma(L) = K(\bigcup_{\sigma \in G} \sigma(L))$ in M enthalten. Wir erhalten also einen Körperturm

$$K \subset K(\bigcup_{\sigma \in G} \sigma(L)) \subset M.$$

Da M/K als Galoiserweiterung separable ist, ist auch $K(\bigcup_{\sigma \in G} \sigma(L))/K$ separabel. Es bleibt also zu zeigen, daß $K(\bigcup_{\sigma \in G} \sigma(L))/K$ normale Erweiterung ist.
Sei $K' \supset K(\bigcup_{\sigma \in G} \sigma(L))$ ein Oberkörper und $\tau : K(\bigcup_{\sigma \in G} \sigma(L)) \to K'$ ein K-Algebrenhomomorphismus. Da die Erweiterung $K(\bigcup_{\sigma \in G} \sigma(L)) \subset M$ endlich ist, denn $K \subset M$ ist endlich, gibt es nach dem Fortsetzungssatz eine endliche Körpererweiterung $M \subset M'$ und einen K-Algebrenhomomorphismus $\tau' : M \to M'$ mit $\tau'\big|_{K(\bigcup_{\sigma \in G} \sigma(L))} = \tau$.

$$\begin{array}{ccccc} K & \hookrightarrow & K(\bigcup_{\sigma \in G} \sigma(L)) & \hookrightarrow & M \\ \| & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \sigma} \\ K & \hookrightarrow & K' & \hookrightarrow & M' \end{array}$$

Da $K \subset M$ endliche normale Erweiterung ist, gilt für den K-Algebrenhomomorphismus $\tau' : M \to M'$, $\tau'(M) = M$. Also ist $\tau' \in G = \mathrm{Gal}(M/K)$. Da G nach dem Hauptsatz der Galoisthoprie eine endliche Gruppe ist, induziert die Multiplikation mit τ' einen Gruppenisomorphismus auf G, insbesondere ist $\tau' G = G$. Damit folgt

$$\tau\left(K(\bigcup_{\sigma \in G} \sigma(L))\right) = K(\tau \bigcup_{\sigma \in G} \sigma(L)) = K(\bigcup_{\sigma \in G} \tau\sigma(L)) = K(\bigcup_{\substack{\alpha = \tau'\sigma \\ \sigma \in G}} \alpha(L)) = K(\bigcup_{\sigma \in G} \sigma(L)).$$

Da auch $K \subset K(\bigcup_{\sigma \in G} \sigma(L))$ endlich ist, ist dies äquivalent dazu, daß $K(\bigcup_{\sigma \in G} \sigma(L))$ normale Erweiterung von K ist.

Aufgabe 4 (F03T2A1)**.** Sei p eine Primzahl mit $p \equiv 1 \mod 4$. Zeigen Sie:

(a) Es gibt eine natürliche Zahl x mit $x^2 \equiv -1 \mod p$.

(b) p ist kein Primelement im Hauptidealring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen.

(c) Es gibt natürliche Zahlen x, y mit $p = x^2 + y^2$.

(6 Punkte)

Lösung. **(a)** Nach dem kleinen Satz von Fermat gilt für $a \neq 0$

$$(a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \mod p.$$

Insbesondere gilt dies für $1 \leqslant a \leqslant \frac{p-1}{2}$. Die natürlichen Zahlen $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ sind paarweise nicht kongruent modulo p, denn gäbe es $1 \leqslant a < b \leqslant \frac{p-1}{2}$ mit $a^2 \equiv b^2 \mod p$, so wäre auch $(p-a)^2 \equiv (-a)^2 \equiv a^2 \mod p$ und da $1 \leqslant a < b \leqslant \frac{p-1}{2} < p - a < p$, hätte das Polynom $X^2 - \overline{a}^2 \in \mathbb{F}_p[X]$ drei verschiedene Nullstellen, Widerspruch.
Das Polynom $X^{\frac{p-1}{2}} - \overline{1} \in \mathbb{F}_p[X]$ hat also genau die $\frac{p-1}{2}$ verschiedenen Nullstellen $\overline{1}^2, \overline{2}^2, \ldots, \left(\overline{\frac{p-1}{2}}\right)^2$.
Da $p \equiv 1 \mod 4$ ist $\frac{p-1}{2}$ gerade, also $(-1)^{\frac{p-1}{2}} \equiv 1 \mod p$.Damit ist auch $-\overline{1} \in \mathbb{F}_p$ Nullstelle des Polynoms $X^{\frac{p-1}{2}} - \overline{1} \in \mathbb{F}_p[X]$. Es folgt, daß es $x \in \{1, \ldots, \frac{p-1}{2}\}$ gibt mit $-1 \equiv x^2 \mod p$.

(b) Angenommen p ist ein Primelement in $\mathbb{Z}[i]$, das heißt (p) ein Primideal und damit maximal. Dann wäre der Quotient $\mathbb{Z}[i]/(p)$ ein Körper. Sei $x \in \mathbb{N}$ das Element aus (a). Die Klasse $\overline{x+i}$ ist $\neq 0$ in $\mathbb{Z}[i]/(p)$, denn sonst gäbe es $a, b \in \mathbb{Z}$ mit $x + i = ap + bpi$, Widerspruch. Ebenso ist die Klasse $\overline{x-i} \neq \overline{0}$. Dann ist

$$(\overline{x+i})(\overline{x-i}) = x^2 - i^2 = -1 - (-1) = 0$$

also $\overline{x+i}$ ein Nullteiler. Widerspruch zur Behauptung, $\mathbb{Z}[i]/(p)$ wäre ein Körper.

(c) Da p nach (b) in $\mathbb{Z}[i]$ kein Primelement ist, lässt sich p schreiben als Produkt von Nichteinheiten

$$p = (x + yi)(w + zi).$$

Der Ring $\mathbb{Z}[i]$ ist bezüglich der Norm $\delta : \mathbb{Z}[i] \to \mathbb{N}, a+bi \mapsto a^2+b^2$ ein euklidischer Ring. Da die euklidische Norm multiplikativ ist folgt

$$p^2 = \delta(p) = \delta(x + yi)\delta(w + zi) = (x^2 + y^2)(w^2 + z^2).$$

Dies ist eine Gleichung in $\mathbb{Z}$, da p Primelement in $\mathbb{Z}$ ist, und $\delta(x + yi) \neq 1 \neq \delta(w + zi)$ folgt $p = x^2 + y^2$ (und ebenso $p = w^2 + z^2$).