Aufgabe 1

(a) Weil L Zerfällungskörper von f über K ist, muss L/K normal sein. Für endliche Körper oder $\operatorname{char} K = 0$ ist L/K separabel. Wegen $(n, \operatorname{char} K) = 1$ gilt $f' = nX^{n-1} \neq 0$ und daher ist L/K separabel. Für beliebige K ist also L/K normal und separabel und damit galoissch. Sei b eine Nullstelle von f. Es gilt $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$ und daher

$$X^n - a = X^n - b^n = b^n((Xb^{-1})^n - 1) = b^n \prod_{\zeta \in \mu_n} (Xb^{-1} - \zeta) = \prod_{\zeta \in \mu_n} (X - \zeta b).$$

Insbesondere gilt $\zeta b \in K(b) \forall \zeta \in \mu_n$, sodass f über $K(b)$ vollständig in Linearfaktoren zerfällt. b liegt als Nullstelle von f notwendigerweise in L. Insgesamt folgern wir $L = K(b)$.

(b) Jedes $\sigma \in \operatorname{Gal}(L/K)$ ist wegen Teilaufgabe (a) eindeutig gegeben durch $\sigma(b)$. Die Menge der Nullstellen hatten wir in (a) bereits bestimmt als $M = \{b\zeta \colon \zeta \in \mu_n\}$. Daher gilt $\operatorname{Gal}(L/K) = \{\sigma_\zeta \colon \zeta \in \mu_n\}$ mit $\sigma_\zeta(b) = \zeta b$. Insbesondere gilt $\psi(\sigma_\zeta) = \frac{\sigma_\zeta(b)}{b} = \zeta \in \mu_n$. Daher hängt ψ nur von der Wahl von $\sigma \in \operatorname{Gal}(L/K)$ ab. Offensichtlich besitzt jedes $\zeta \in \mu_n$ ein Urbild unter ψ, sodass wir $\operatorname{im} \psi = \mu_n$ folgern können. Weiterhin gilt

$$\psi(\sigma_\zeta \sigma_{\zeta'}) = \frac{\sigma_\zeta(\sigma_{\zeta'}(b))}{b} = \frac{\sigma_\zeta(\zeta' b)}{b} = \frac{\zeta' \sigma_\zeta(b)}{b} = \zeta' \zeta.$$

Es handelt sich also um einen Gruppenhomomorphismus. Für die Injektivität genügt es zu zeigen, dass $\ker \psi = \{\mathrm{id}\}$. Das folgt aber sofort aus $\psi(\sigma) = 1 \Leftrightarrow \sigma(b) = b \Leftrightarrow \sigma = \mathrm{id}$. Wir erhalten daher einen Gruppenisomorphismus $\psi \colon \operatorname{Gal}(L/K) \xrightarrow{\sim} \mu_n$. Da μ_n zyklisch ist, muss auch $\operatorname{Gal}(L/K)$ zyklisch sein.

(c) Für ein Gegenbeispiel siehe Aufgabe 2 auf Zettel 8. Dort gilt $K = \mathbb{Q}$, $n = 4$, $f = X^4 - 2$, $\mu_n = \{1, -1, i, -i\} \subsetneq \mathbb{Q}$ und $\operatorname{Gal}(L/K) \cong D_4$. D_4 ist aber nicht zyklisch.

Aufgabe 2

(a) Wir zeigen zunächst, dass jedes $\begin{pmatrix} e \\ f \end{pmatrix} \in V$ eine Darstellung $g \cdot m$ mit $g \in G, m \in M$ besitzt. Dazu unterscheiden wir drei Fälle

(1) $f \neq 0$. Dann gilt

$$\begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} 1 & e \\ 0 & f \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(2) $f = 0, e \neq 0$. Dann gilt

$$\begin{pmatrix} e \\ 0 \end{pmatrix} = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

(3) $f = e = 0$. Dann gilt

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Nun müssen wir zeigen, dass die von $m, n \in M$ erzeugten Bahnen für $n \neq m$ disjunkt sind. Es gilt aufgrund der Linearität

$$G\begin{pmatrix}0\\0\end{pmatrix} = \left\{g\begin{pmatrix}0\\0\end{pmatrix} : g \in G\right\} = \left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}.$$

Da alle Matrizen aus $G \subset \mathrm{GL}_2(\mathbb{F}_p)$ invertierbar sind, gilt außerdem

$$\begin{pmatrix}0\\0\end{pmatrix} \notin G\begin{pmatrix}0\\1\end{pmatrix} \qquad \text{und} \qquad \begin{pmatrix}0\\0\end{pmatrix} \notin G\begin{pmatrix}1\\0\end{pmatrix}.$$

Es verbleibt zu zeigen, dass $G\begin{pmatrix}0\\1\end{pmatrix} \cap G\begin{pmatrix}1\\0\end{pmatrix} = \emptyset$. Nehmen wir an $\exists g \in G$ mit

$$\begin{pmatrix}1\\0\end{pmatrix} = g\begin{pmatrix}0\\1\end{pmatrix} \implies \exists a, b, d \in \mathbb{F}_p, a \neq 0, d \neq 0\colon \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a & b\\0 & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}b\\d\end{pmatrix}$$

so erhalten wir durch Komponentenvergleich $d = 0$, Widerspruch. Nehmen wir stattdessen an $\exists g \in G$ mit

$$\begin{pmatrix}0\\1\end{pmatrix} = g\begin{pmatrix}1\\0\end{pmatrix} \implies \exists a, b, d \in \mathbb{F}_p, a \neq 0, d \neq 0\colon \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a & b\\0 & d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a\\0\end{pmatrix},$$

so erhalten wir durch Komponentenvergleich $a = 0$, Widerspruch. Daher zerfällt V in die disjunkte Vereinigung der durch Gruppenoperation von G aus $m \in M$ erzeugten Teilmengen, M ist also eine Repräsentantensystem der Bahnen.

(b) Sei $x = \begin{pmatrix}e\\f\end{pmatrix} \in V$. Wir unterscheiden drei Fälle

(1) $f \neq 0$. Für $\begin{pmatrix}a & b\\0 & d\end{pmatrix} \in G_x$ gilt dann

$$\begin{pmatrix}e\\f\end{pmatrix} = \begin{pmatrix}a & b\\0 & d\end{pmatrix}\begin{pmatrix}e\\f\end{pmatrix} = \begin{pmatrix}ae + bf\\df\end{pmatrix} \Leftrightarrow d = 1 \wedge ae + bf = e \Leftrightarrow d = 1 \wedge b = (1-a)e \cdot f^{-1}$$

Daraus folgt

$$G_x = \left\{\begin{pmatrix}a & (1-a)e \cdot f^{-1}\\0 & 1\end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p), a \neq 0\right\}.$$

Insbesondere gilt $\#G_x = p - 1$, da ein Vertreter von G_x durch $a \in \mathbb{F}_p^\times$ bereits eindeutig bestimmt ist.

(2) $f = 0, e \neq 0$. Für $\begin{pmatrix}a & b\\0 & d\end{pmatrix} \in G_x$ gilt dann

$$\begin{pmatrix}e\\0\end{pmatrix} = \begin{pmatrix}a & b\\0 & d\end{pmatrix}\begin{pmatrix}e\\0\end{pmatrix} = \begin{pmatrix}ae\\0\end{pmatrix} \Leftrightarrow e = ae \Leftrightarrow a = 1.$$

Wir erhalten daher

$$G_x = \left\{\begin{pmatrix}1 & b\\0 & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p), d \neq 0\right\}.$$

Insbesondere ist $\#G_x = p \cdot (p-1)$.

(3) Für $x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ist die Isotropiegruppe wegen $G\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}$ durch ganz G gegeben.

(c) Es gilt $\#G = (p-1)\cdot p\cdot(p-1)$, da es jeweils $p-1$ Möglichkeiten für a und d und p Möglichkeiten für b gibt. Sei $x = \begin{pmatrix} e \\ f \end{pmatrix} \in V$. Wir unterscheiden wieder drei Fälle

(1) $f \neq 0$. Wegen
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} ae + bf \\ df \end{pmatrix}$$
und $df \neq 0$ gilt $Gx \subset \mathbb{F}_p \times \mathbb{F}_p^\times$. ($df \neq 0$ folgt wegen $d \neq 0$, $f \neq 0$).
Da $\mathbb{F}_p$ ein Körper ist, gilt außerdem für beliebige $a \in \mathbb{F}_p, b \in \mathbb{F}_p^\times$
$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & (a-e)f^{-1} \\ 0 & bf^{-1} \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} e + (a-e)f^{-1}f \\ bf^{-1}f \end{pmatrix} \in Gx.$$
Daraus folgt sofort die Gleichheit $Gx = \mathbb{F}_p \times \mathbb{F}_p^\times$. Insbesondere gilt $\#Gx = p\cdot(p-1)$. Damit erhalten wir
$$\#Gx \cdot \#G_x = p\cdot(p-1)\cdot(p-1) = \#G.$$

(2) $e \neq 0, f = 0$. Wegen
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} e \\ 0 \end{pmatrix} = \begin{pmatrix} ae \\ 0 \end{pmatrix}$$
und $ae \neq 0$ gilt $Gx \subset \mathbb{F}_p^\times \times \{0\}$. ($ae \neq 0$ folgt wegen $a \neq 0$, $e \neq 0$).
Da $\mathbb{F}_p$ ein Körper ist, gilt außerdem für beliebiges $a \in \mathbb{F}_p$
$$\begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} ae^{-1} & b \\ 0 & d \end{pmatrix} \begin{pmatrix} e \\ 0 \end{pmatrix} \in Gx.$$
Daraus schließen wir die Gleichheit $Gx = \mathbb{F}_p^\times \times \{0\}$. Insbesondere gilt $\#Gx = p-1$. Damit erhalten wir $\#Gx \cdot \#G_x = (p-1)\cdot(p-1)\cdot p = \#G$.

(3) $e = f = 0$. Wie oben gezeigt ist dann $Gx = \{x\}$ und $G_x = G$. Es gilt also $\#G_x \cdot \#(Gx) = \#G \cdot \#\{x\} = \#G$.

(d) Nach Lemma 5.10 gilt $(G\colon G_x) = \#Gx$. Wir betrachten die drei Elemente von M.

(1) $x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Es gilt $(G\colon G_x) = \#Gx = p\cdot(p-1)$ (siehe (c), Fall 1).

(2) $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Es gilt $(G\colon G_x) = \#Gx = (p-1)$ (siehe (c), Fall 2).

(3) $x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Es gilt $(G\colon G_x) = \#Gx = 1$ (siehe (c), Fall 3).

Insgesamt erhalten wir
$$\sum_{x\in M} (G\colon G_x) = p\cdot(p-1) + p - 1 + 1 = p^2 = \#\mathbb{F}_p^2 = \#V.$$

Aufgabe 3

(a) Die Anzahl s der 101-Sylowgruppen teilt $2020 = 2^2 \cdot 5 \cdot 101$. Außerdem gilt $s \equiv 1 \mod 101$. Allerdings gilt für jeden Teiler d von 2020 mit $d > 20$ sofort $101|d$, also $d \equiv 0 \mod 101$. Daraus folgt $s = 1$. Wir bezeichnen die eindeutig bestimmte 101-Sylowgruppe mit S. Nach Bemerkung 5.30 und wegen $2020 = 20 \cdot 101$ mit $(20, 101) = 1$ folgt $\#S = 101$. G operiert durch Konjugation auf seinen Untergruppen. gSg^{-1} ist daher eine Untergruppe von G und wegen $\#gSg^{-1} = \#S = 101$ ist gSg^{-1} eine 101-Gruppe. Nach Satz 5.29 existiert dann eine 101-Sylowgruppe S' mit $gSg^{-1} \subset S'$. Es gibt aber nur eine 101-Sylowgruppe, $S = S'$. Insbesondere ist also $S \in \mathrm{Fix}_G(\{H \text{ Untergruppe in } G\}) \Leftrightarrow S \triangleleft G$ wegen Lemma 5.18. Da $\#S$ prim ist, muss S kommutativ sein. Also ist S der gesuchte kommutative nicht-triviale Normalteiler.

(b) Es gilt $43 < 47$ und $43 \nmid 47 - 1$. Nach Korollar 5.34 ist jede Gruppe der Ordnung $2021 = 43 \cdot 47$ zyklisch und insbesondere abelsch. Nach dem Hauptsatz für endliche abelsche Gruppen ist daher jede Gruppe der Ordnung 2021 isomorph zu $\mathbb{Z}/2021\mathbb{Z}$.

(c) Die Anzahl s der 3-Sylowgruppen teilt $36 = 2^2 \cdot 3^2$. Außerdem gilt $s \equiv 1 \mod 3$. Daher gilt $3 \nmid s$. Wir erhalten die zwei Möglichkeiten $s = 1$ oder $s = 4$.

Für $s = 1$ argumentieren wir analog wie in Teilaufgabe (a): Wir bezeichnen die eindeutig bestimmte 3-Sylowgruppe mit S, dann gilt $S \in \mathrm{Fix}_G(\{H \text{ Untergruppe in } G\}) \Leftrightarrow S \triangleleft G$. S hat die Ordnung 9, da $36 = 4 \cdot 9$ mit $(4, 9) = 1$. In diesem Fall existiert also ein nicht-trivialer Normalteiler.

Ist nun $s = 4$, so gibt es vier verschiedene 3-Sylowgruppen. Wie oben bewiesen ist für eine p-Sylowgruppe S auch gSg^{-1} eine p-Sylowgruppe. Daher operiert G vermöge der Konjugation auf der Menge X ihrer 3-Sylowgruppen. Wir betrachten daher den analog zu Beispiel 5.2 3) von der Konjugation induzierten Homomorphismus

$$\varphi\colon G \to \mathfrak{S}(X) \cong \mathfrak{S}_4 \tag{1}$$
$$g \mapsto \tau_g \tag{2}$$

Nun gilt wegen $\operatorname{im}\varphi \subset \mathfrak{S}(X)$ auch $\#\operatorname{im}\varphi < 24$, φ kann also nicht injektiv sein und wir erhalten $\ker\varphi \neq \{1\}$. Wäre $\ker\varphi = G$, so wäre $\operatorname{im}\varphi = \mathrm{id}$. Da es aber vier verschiedene zueinander konjugierte Untergruppen gibt, können wir diesen Fall auch ausschließen. Damit ist $\ker\varphi$ der gesuchte nichttriviale Normalteiler.

Aufgabe 4

Def. 1. Zwei Transpositionen (a, b) und (c, d) heißen disjunkt, wenn $\{a, b\} \cap \{c, d\} = 0$ gilt.

(a) Sei $n \in \{1, \ldots, n\}$. Wir unterscheiden zwei Fälle.

(1) $n = \sigma(x_i)$ für ein $i \in \{1, \ldots, r\}$. Dann gilt

$$\sigma(x_1, \ldots, x_r)\sigma^{-1}(n) = \sigma(x_1, \ldots, x_r)(x_i) = \sigma(x_{i+1}).$$

(2) $n \neq \sigma(x_i) \forall i \in \{1, \ldots, r\}$. Dann gilt

$$\sigma(x_1, \ldots, x_r)\sigma^{-1}(n) = \sigma(\sigma^{-1}(n)) = n.$$

Insgesamt erhalten wir daher

$$\sigma(x_1, \dots, x_r)\sigma^{-1} = (\sigma(x_1), \dots, \sigma(x_n)).$$

(b) Für $\tau \in \mathfrak{V}_4$ gilt $\tau = \tau_1\tau_2$ für zwei disjunkte Transpositionen τ_1 und τ_2. Wir folgern $\sigma\tau\sigma^{-1} = \sigma\tau_1\sigma^{-1}\sigma\tau_2\sigma^{-1} = \tau_1'\tau_2'$ für zwei Zyklen τ_1' und τ_2'. Permutationen erhalten Disjunktheit von Mengen, also insbesondere auch Disjunktheit von Transpositionen. Daher sind τ_1' und τ_2' ebenfalls disjunkt. $\mathfrak{V}_4$ enthält aber bereits alle möglichen Kompositionen von zwei disjunkten Zyklen in $\mathfrak{S}_4$. Daher gilt $\sigma\tau\sigma^{-1} \in \mathfrak{V}_4 \forall \tau \in \mathfrak{V}_4$. Folglich ist $\mathfrak{V}_4$ ein Normalteiler in $\mathfrak{S}_4$.

(c) $1 \triangleleft \mathfrak{V}_4$ ist trivial. $\mathfrak{V}_4$ ist Normalteiler in $\mathfrak{S}_4$, also insbesondere auch in $\mathfrak{A}_4$. $\mathfrak{A}_4$ ist als Kern des Gruppenhomomorphismus $\operatorname{sgn}\colon \mathfrak{S}_4 \to \{1, -1\}$ Normalteiler in $\mathfrak{S}_4$. $1 \triangleleft \mathfrak{V}_4 \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4$ bildet daher eine Normalreihe. Es gilt $(\mathfrak{S}_4 : \mathfrak{A}_4) = 2$. Jede Gruppe der Ordnung 2 ist abelsch, da ein Element das neutrale Element ist. Außerdem gilt $\#\mathfrak{A}_4 = 12$, $\#\mathfrak{V}_4 = 4$ und damit $(\mathfrak{A}_4 \colon \mathfrak{V}_4) = 3$. Eine Gruppe der Ordnung drei besitzt die Elemente e, a und b. e kommutiert mit allen Gruppenelementen. Da jedes Element ein Inverses besitzen muss und wegen $a \neq e \implies a^{-1} \neq e$ gilt weiter $ab = e = ba$. Folglich ist $\mathfrak{A}_4/\mathfrak{V}_4$ abelsch. Schließlich müssen wir noch nachweisen, dass $\mathfrak{V}_4$ abelsch ist. Da Transpositionen kommutieren, ist dies aber sofort klar. Per Definition ist $\mathfrak{S}_4$ daher auflösbar.