Aufgabe 1 (???)**.** Sei K ein Körper. Man zeige: Jede endliche Untergruppe von $(K\backslash\{0\},\cdot)$ ist zyklisch.

Lösung. Sei $G \subset K \setminus \{0\}$ eine endliche Untergruppe und m ihr Exponent.
Erinnerung: Für eine beliebige endliche Gruppe G ist der Exponent die Zahl $m = \min\{k \in \mathbb{N} \bigm| \forall x \in G : x^k = e\}$.
Wir zeigen zuerst, daß es $x \in G$ gibt mit $\mathrm{ord}(x) = m$. Sei $|G| = n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, $r \in \mathbb{N}_0$, Primzahlen $p_1 < \cdots < p_r$, und $\nu_i \in \mathbb{N}$. Nach dem Hauptsatz über endliche abelsche Gruppen gibt es $b_{ij} \in G$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s_i$, und natürliche Zahlen $k_{i1} \geqslant \ldots \geqslant k_{is_i} \geqslant 1$ mit

$$G = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s_i} \mathbb{Z}\, b_{ij} \quad \text{und } \mathrm{ord}(b_{ij}) = p_i^{k_{ij}} \text{ für } 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s_i.$$

Es gilt: $m = p_1^{k_{1,1}} \cdots p_r^{k_{r,1}}$. Sei $x = b_{11} + \cdots + b_{r1}$. Es gilt $\mathrm{ord}(x) = m$, denn für $z \in \mathbb{Z}$ gilt

$$zx = 0 \Leftrightarrow \forall i \in \{1, \ldots, r\} : zb_{i1} = 0 \Leftrightarrow \forall i : p_i^{k_{i1}} \big| z \Leftrightarrow m \big| z.$$

Es gilt $x^m = 1$ für alle $x \in G$. Da das Polynom $X^m - 1 \in K[X]$ höchstens m Nullstellen in K hat, gilt $|G| \leqslant m$. Da auch $m \big| |G|$ ist, folgt $|G| = m$, also ist G zyklisch.

Aufgabe 2 (Frühjahr 1984)**.** Sei G eine Gruppe mit der Einsuntergruppe 1 und $P = G \times G$ das direkte Produkt von G mit sich selbst. Es sei $G_1 = G \times 1$ und $G_2 = 1 \times G$. Zeigen Sie:

(a) Die Diagonale $D = \{(g, g); g \in G\}$ ist eine Untergruppe von P.

(b) Für jede Untergruppe U zwischen D und P gilt: $U \cap G_i$ ist normal in G_i für $i = 1, 2$.

(c) Genau dann ist D eine maximale Untergruppe von P, wenn G einfach ist.

Lösung. **(a)** Das direkte Produkt P ist eine Gruppe bezüglich der komponentenweisen Multiplikation, dh. $(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$; das neutrale Element ist $(1, 1)$, wobei $1 \in G$ das neutrale Element ist; das Inverse wird komponentenweise gebildet, dh. $(x, y)^{-1} = (x^{-1}, y^{-1})$. Für die Diagonale gilt nach Definition $(1, 1) \in D$. Außerdem ist für $(x, x), (y, y) \in D$ auch $(x, x)(y, y) = (xy, xy) \in D$. Letztlich ist für $(x, x) \in D$ auch $(x, x)^{-1} = (x^{-1}, x^{-1}) \in D$. Damit ist $D \subset P$ eine Untergruppe.

(b) Sei $D \subset U \subset P$. Wir haben zu zeigen, daß $U \cap G_i \triangleleft G_i$.
(Beobachtungen: $D \cap G_i = \{(1, 1)\}$. Außerdem für $(g, g) = (g, 1)(1, g)$.)
Setze $U_i = U \cap G_i$. OBdA. führen wir den Beweis für $i = 1$, der Fall $i = 2$ funktioniert analog. Für $(g, 1) \in G_1$ zeigen wir, daß $(g, 1)U_1(g, 1)^{-1} \subset U$. Sei also $(u, 1) \in U_1$. Dann ist

$$(g, 1)(u, 1)(g, 1)^{-1} = (g, 1)(u, 1)(g^{-1}, 1) = (gug^{-1}, 1) \in G \times 1 = G_1.$$

Andererseits ist auch

$$(gug^{-1}, 1) = (gug^{-1}, gg^{-1}) = (g, g)(u, 1)(g^{-1}, g^{-1}) \in U,$$

da $(g, g), (g^{-1}, g^{-1}) \in D \subset U$, und $(u, 1) \in U$ nach Voraussetzung. Also ist $(g, 1)(u, 1)(g, 1)^{-1} \in G_1 \cap U = U_1$.

(c) Vorbemerkung: Die Abbildungen $q_i : G \to P = G \times G$ sind injektive Gruppenhomomorphismen. Also sind $q_i : G \to G_i$ Isomorphismen und G ist genau dann einfach, wenn die G_i einfach sind.
„$\Rightarrow$“: Sei D eine maximale Untergruppe. Die Untergruppe G_1 (ebenso wie die Untergruppe G_2) ist Normalteiler von P nach Definition des direkten Produkts. Betrachte das Komplexprodukt $G_1D = \{x \in P \mid \exists g_1 \in G_1, d \in D : x = g_1d\}$. Es gilt automatisch $G_1D \subset P$. Andererseits auch $P \subset G_1D$, da $(x_1, x_2) = (x_1x_2^{-1}, 1)(x_2, x_2)$. Also $G_1D = P$ Genauso sieht man $DG_1 = P$. Wir haben bereits gesehen, daß $D \cap G_1 = \{(1, 1)\}$. Sei $\kappa : D \to \mathrm{Aut}(G_1)$ definiert durch die Konjugation und $G_1 \times_\kappa D$ das entsprechende semidirekte Produkt. Dann ist

$$f : G_1 \times_\kappa D \to P, ((g, 1), (d, d)) \mapsto (gd, d)$$

ein Gruppenisomorphismus.

Wäre nun G nicht einfach, so gäbe es $N \lhd G$, und $N_1 = N \times 1 \lhd G_1$. Dann wäre $N_1 \times_\kappa D \subset G_1 \times_\kappa D$ eine echte Untergruppe, die $1 \times_\kappa D$ enthält. Und $D \subsetneq f(N_1) \subsetneq P$, Widerspruch.
„$\Leftarrow$": Sei $D \subset U \subset P$ eine Untergruppe. Dann ist $U_i \lhd G_i$. Da aber G_i einfach ist, folgt $U_i = G_i$ oder $U_i = \{(1,1)\}$.

1. Fall: Ist $U_1 = G_1$ und $U_2 = G_2$, so ist $U = U_1U_2 = G_1G_2 = P$.
2. Fall: Ist $U_1 = \{(1,1)\} = U_2$, so ist $U = D$.
3. Fall: Ist $U_1 = G_1$ und $U_2 = \{(1,1)\}$, so ist $U = G_1$. Da aber $D \subset U$, folgt $G = 1$,und damit trivial, Widerspruch zur Einfachheit.
4. Fall: Genauso falls $U_2 = G_2$ und $U_1 = \{(1,1)\}$.

Aufgabe 3 (Frühjahr 1995)**.** Seien E, G Gruppen und $\pi : E \to G$ ein Epimorphismus. π heißt *zerfallend*, falls ein Homomorphismus $\rho : G \to E$ mit $\pi\rho = \mathrm{id}_G$ existiert.
Zeigen Sie: Ist π ein zerfallender Epimorphismus mit Kern K, so ist

$$K \times G \to E, (k,g) \mapsto k\rho(g) \quad \text{für alle } k \in K \text{ und } g \in G,$$

ein Isomorphismus, falls $K \times G$ mit der Gruppenstruktur des semidirkten Produktes bezüglich einer passenden Operation von G auf K versehen wird.

Lösung. Da $K = \ker(\pi)$, ist $K \lhd E$ ein Normalteiler, und $\rho(G) \subset E$ eine Untergruppe. Daher macht es Sinn eine Operation von G auf K zu definieren durch die Konjugation von $\rho(G)$ auf K:

$$\kappa : G \to \mathrm{Aut}(K), \kappa(g)(k) = \rho(g)k\rho(g)^{-1}.$$

Wir betrachten nun das semidirekte Produkt $K \times_\kappa G$ mit

Multiplikation: $(k_1, g_1)(k_2, g_2) = (k_1\kappa(g_1)(k_2), g_1g_2) = (k_1\rho(g_1)k_2\rho(g_1)^{-1}, g_1g_2)$,

neutralem Element: (e_K, e_G),

Inversem: $(k,g)^{-1} = (\kappa(g^{-1})k^{-1}, g^{-1}) = (\rho(g)^{-1}k^{-1}\rho(g), g^{-1})$.

Damit ist die Abbildung $f : K \times_\kappa G \to E, (k,g) \mapsto k\rho(g)$ ein Homomorphismus, denn

$$f((k_1,g_1)(k_2,g_2)) = f(k_1\rho(g_1)k_2\rho(g_1)^{-1}, g_1g_2) = k_1\rho(g_1)k_2\rho(g_1)^{-1}\rho(g_1g_2) = k_1\rho(g_1)k_2\rho(g_2) = f(k_1,g_1)f(k_2,g_2).$$

Um zu zeigen daß f injektiv ist, beobachten wir, daß $K \cap \rho(G) = \{e_E\}$. Sei nämlich $x \in K \cap \rho(G)$. Das heißt, es gibt $g \in G$ mit $x = \rho(g)$. Andererseits ist $\pi(x) = e_G$, also $e_G = \pi(x) = \pi(\rho(g)) = \mathrm{id}_G(g) = g$, also $x = \rho(e_G) = e_E$, und $K \cap \rho(G) = \{e_E\}$ wie gewünscht. Es gilt nun

$$\begin{aligned} f(k,g) = e_E \quad &\Rightarrow \quad k\rho(g) = e_E \quad \Rightarrow \quad k = \rho(g)^{-1} \in K \cap \rho(G) = \{e_E\} \quad \Rightarrow \quad k = \rho(g) = e_E \\ &\Rightarrow \quad k = e_E,\ g = \pi\rho(g) = \pi(e_E) = e_G \quad \Rightarrow \quad (k,g) = (e_E, e_G). \end{aligned}$$

Zeigen wir nun, daß f surjektiv ist. Sei $x \in G$, und $g := \pi(x)$. Dann ist $k := x\rho(g)^{-1} \in K$, denn $\pi(x\rho(g)^{-1}) = \pi(x)\pi\rho(g)^{-1} = gg^{-1} = e_G$. Wir berechnen

$$f(k,g) = k\rho(g) = x\rho(g)^{-1}\rho(g) = x,$$

dh. f ist surjektiv.
Insgesamt haben wir gezeigt, daß f ein Isomorphismus ist.

Aufgabe 4. Bestimmen Sie bis auf Isomorphie alle abelschen Gruppen der Ordnung 2019.

Lösung. Wir kennen bereits die Primfaktorzerlegung von 2019:

$$2019 = 673 \cdot 3.$$

Nach dem Hauptsatz über endliche abelsche Gruppen gibt es bis auf Isomorphie genau eine Gruppe der Ordnung 2019, nämlich

$$\mathbb{Z}/2019\,\mathbb{Z} \cong \mathbb{Z}/673\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z}.$$

Aufgabe 5 (Frühjahr 1996). (a) Wie viele Isomorphieklassen von abelschen Gruppen der Ordnung 64 gibt es?

(b) Bestimmen Sie die kleinste natürliche Zahl n, so daß es genau sechs Isomorphieklassen von abelschen Gruppen der Ordnung n gibt.

Lösung. **(a)** Es ist $64 = 2^6$. Die Anzahl der bis auf Isomorphie verschiedenen abelschen Gruppen der Ordnung 64 ist gleich der Anzahl der Folgen $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_r \geqslant 1$ mit $m_1 + \ldots m_r = 6$ (nach dem Hauptsatz über endliche abelsche Gruppen).

$$\begin{aligned} 6 &= 1+1+1+1+1+1 \\ &= 2+1+1+1+1 \\ &= 2+2+1+1 \\ &= 2+2+2 \\ &= 3+1+1+1 \\ &= 3+2+1 \\ &= 3+3 \\ &= 4+1+1 \\ &= 4+2 \\ &= 5+1 \\ &= 6 \end{aligned}$$

Also gibt es bis auf Isomorphie genau 11 abelsche Gruppen der Ordnung 64.

(b) Wir verwenden den Hauptsatz über endliche abelsche Gruppen. Für eine Primzahl p gibt es genau zwei Isomorphieklassen von Gruppen der Ordnung p^2: $\mathbb{Z}/p^2$ und $\mathbb{Z}/p \times \mathbb{Z}/p$ und drei Isomorphieklassen der Ordnung p^3: $\mathbb{Z}/p^3$, $\mathbb{Z}/p^2 \times \mathbb{Z}/p$ und $\mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$, denn

$$2 = 1+1 \quad \text{und} \quad 3 = 1+1+1 = 2+1$$

Um auf 6 zu kommen, müssen wir ein Produt aus zwei verschiedenen Primzahlen wählen. Sei also $p = 2$ und $q = 3$, und $n = 2^3 3^2 = 72$. Es gibt sechs Isomorphieklassen der Ordnung 72.

Aufgabe 6 (Herbst 2001). (a) G sei eine endliche abelsche Gruppe, p das Produkt aller Elemente von G. Zeigen Sie:

$$p = \begin{cases} 1 & \text{falls } G \text{ kein oder mehr als ein Element der Ordnung 2 hat} \\ \text{a} & \text{sonst, wobei } a \text{ dann das einzige Element der Ordnung 2 von } G \text{ ist.} \end{cases}$$

(b) Zeigen Sie: Jede natürliche Zahl $n \neq 4$ teilt die Zahl $((n-1)!)^2 + (n-1)!$.

Lösung. **(a)** Hat ein Element $x \in G$ die Ordnung 2, so gilt $x^2 = 2$ oder anders gesagt $x = x^{-1}$. Für alle anderen Elemente gilt $x \neq x^{-1}$.
In dem Produkt p fassen wir nun jeweils die beiden Elemente zusammen, die invers zueinander sind, so daß sie 1 ergeben, also

$$p = \prod_{x \in G} x = \prod_{\substack{x \in G \\ \operatorname{ord} x = 2}} x.$$

Gibt es in G keine Elemente der Ordnung zwei, so folgt $p = 1$. Gibt es genau ein Element $a \in G$ der Ordnung zwei, so folgt $p = a$.
Angenommen, es gibt in G paarweise verschiedene Elemente $a_1, \ldots, a_m$, $m \geqslant 2$, der Ordnung 2. Wir zeigen, daß das Produkt $a = a_1 \cdots a_m$ immer $= 1$ sein muß.Das Produkt $a_1 a_2$ hat Ordnung 2, und kann nicht $1, a_1, a_2$ sein. Also gibt es $i \in \{3, \ldots m\}$ mit $a_1 a_2 = a_i$. Da a_i aber bereits an anderer Stelle des PRodukts vorkommt, und $a_i^2 = 1$ erhalten wir eine Darstellung von a als Produkt mit $m - 3$ Elementen. Nun fährt man so fort, das Produkt zu verkürzen. Ist $a_i a_{i+1} = a_j$ wobei a_j noch weiter hinten im Produkt vorkommt, so kann man die Darstellung um 3 Elemente verkürzen. Ist $a_i a_{i+1} = a_j$ wobei man a_j bereits

eliminiert hat, so kann man wenigstens $a_i a_{i+1}$ durch a_j ersetzten und verkürzt die Dartstellung um ein Element. Man kann sich leicht überlegen, daß man so schließlich erhält $a = a_1 \cdots a_m = 1$.

(b) Sei $n = p > 2$ eine Primzahl, dann ist $\mathbb{Z}/p\mathbb{Z}^\times$ eine zyklische Gruppe der Ordnung $p-1$ mit genau einem Element der Ordnung 2, nämlich $-1 \equiv p-1 \mod p$. Nach **(a)** folgt $(p-1)! \equiv -1 \mod p$, also $((p-1)!)^2 + (p-1)! \equiv (-1)^2 - 1 \equiv 0 \mod p$, und damit $p|((p-1)!)^2 + (p-1)!$.
Der Fall $p = 2$ ist trivial.
Sei n nicht prim, schreibe $n = p_1^{k_1} \cdots p_m^{k_m}$ mit paarweise verschiedenen Primzahlen p_i. Jeder echte Teiler von n teilt $(n-1)!$, insbesondere dann $p_i^{k_i}|(n-1)!$ falls $m > 1$, also $n|(n-1)!$. Falls $m = 1$ und $k_1 \geqslant 2$, so sieht man leicht, daß sowohl $p_1^{k_1-1}$ und p das Procukt $(p_1^{k_1} - 1)!$ teilen. Isngesamt $n|(n-1)!$ und

$$n|((n-1)!)^2 + (n-1)! = (n-1)!\,((n-1)! + 1)\,.$$