Wahr oder Falsch?

✓ In jeder p-Gruppe gibt es ein Element der Ordnung p.
Falsch: Sei $p^{825853333}-1$. Die triviale Gruppe hat Ordnung $1 = p^0$, ist also eine p-Gruppe, hat aber keine Elemente der Ordnung p.

$\mathbb{Z}/4\mathbb{Z}$ ist kein semidirektes Produkt $N \rtimes H$ mit $N, H \neq \{0\}$
Wahr: Wäre $\mathbb{Z}/4\mathbb{Z}$ ein semidirektes Produkt, müsste es einen Normalteiler N von $\mathbb{Z}/4\mathbb{Z}$ und eine Untergruppe H von $\mathbb{Z}/4\mathbb{Z}$ geben, sodass $N+H = \mathbb{Z}/4\mathbb{Z}$ und $N \cap H = \{0\}$. Es gibt aber nur genau eine echte Untergruppe von $\mathbb{Z}/4\mathbb{Z}$ und zwar $N = \langle 2 \rangle$

✓ 7 hat eine Quadratwurzel in $\mathbb{F}_{11}$.
F: $\left(\frac{7}{11}\right) = (-1)^{3\cdot 5}\left(\frac{11}{7}\right) = (-1)\left(\frac{4}{7}\right) = (-1)\left(\frac{2}{7}\right)\left(\frac{2}{7}\right) = -1$

✓ Sei R ein Integritätsbereich und $p \in R$ prim. Dann ist $R/(p)$ ein Körper.
Falsch: $2 \in \mathbb{Z}[x]$ ist prim, aber $\mathbb{Z}[x]/(2) \cong \mathbb{Z}/2\mathbb{Z}[x]$ ist kein Körper.

$\mathbb{Z}[x]$ ist ein Integritätsbereich, da Teilmenge.

✓ Die Gruppen $\mathbb{Z}/36\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ sind isomorph.
Falsch: Das Element $[1] \in \mathbb{Z}/36\mathbb{Z}$ hat die Ordnung 36. In $(\mathbb{Z}/6\mathbb{Z})^2 := \mathbb{Z}$ hingegen existiert kein Element mit dieser Ordnung, da für jeden $g \in \mathbb{Z}$ die Ordnung ein Teiler von 6 sein muss. Insbesondere $\mathrm{ord}(g) \leq 6 \ \forall g \in \mathbb{Z}$.

3333 ist die Summe von zwei Quadraten in $\mathbb{N}$!
Falsch: Nach dem Satz von Fermat ist eine positive ganze Zahl n genau dann die Summe zweier Quadrate in $\mathbb{N}$, wenn jede Primzahl p mit $p \equiv -1 \bmod 4$ die Zahl n mit gerader Vielfachheit teilt. $3333 = 3 \cdot 11 \cdot 101$ und $11 \equiv -1 \bmod 4$, aber 11 teilt 3333 mit ungerader Vielfachheit.

✓ Jede p-Gruppe ist abelsch.
Falsch: Zum Beispiel haben die Diedergruppe D_4 und die Quaternionengruppe $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ Ordnung 8, sind also 2-Gruppen. Beide sind nicht abelsch, denn in D_4 gilt $rs = sr^{-1} = sr^3 \neq sr$ und in Q gilt $ij = -ji \neq ji$. $ds = sd^{-1} = sd^3 \neq sd$

✓ Jede kommutative Ring ist isomorph zu einem Unterring eines Körpers.
Falsch: Jeder Unterring eines Körpers ist nullteilerfrei, aber nicht jeder Ring ist nullteilerfrei. Zum Beispiel $\mathbb{Z}/n\mathbb{Z}$ ($n > 1$ nicht prim).

✓ Das Nullideal (0) eines Rings R ist genau dann ein Primideal, wenn R nullteilerfrei ist.
Richtig: Nullideal ist Primideal
$\Leftrightarrow ab \in (0) \Rightarrow a \in (0) \vee b \in (0)$ ⇕
R ist Nullteilerfrei
$\Leftrightarrow ab = 0 \Rightarrow a = 0 \vee b = 0$

✓ Für je zwei Primzahlen p und q mit $p, q \equiv 3 \bmod 4$ gilt: p ist genau dann quadratischer Rest mod. q, wenn q quadratischer ~~Rest~~ Nichtrest mod p ist.
Richtig: p ist genau dann quadratischer Rest mod. q, wenn $\left(\frac{p}{q}\right) = 1$ ist. Umgekehrt ist q genau dann quadratischer Nichtrest mod p wenn $\left(\frac{q}{p}\right) = -1$ ist. Nach dem quadratischen Reziprozitätsgesetz ist $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$ und das Vorzeichen $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ ist negativ, da $p, q \equiv 3 \bmod 4$.

✓ Sei $N \trianglelefteq G$ ein Normalteiler der Gruppe G. Dann gibt es eine weitere Gruppe H und einen Gruppenhom. $\varphi: G \to H$ mit $\ker(\varphi) = N$.
Wahr: Es sei $H := G/N$ die Faktorgruppe und $\varphi: G \to H, g \mapsto gN$ die kanonische Surjektion. Dann ist $N = \ker(\varphi)$, denn $\ker(\varphi) = \{g \in G \mid gN = N\}$.

✓ Sei G eine endliche abelsche Gruppe, sodass jede Primzahl $p \in \mathbb{N}$ die Ordnung $|G|$ höchstens einmal teilt. Dann ist G zyklisch.

Wahr: Es sei $|G| = p_1 \cdot p_2 \cdots p_m$ mit $p_1 < p_2 < \dots < p_m \in \mathbb{P}$. Nach dem Klassifikationssatz für endliche abelsche Gruppen ist G isomorph zu $\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \dots \times \mathbb{Z}/p_m\mathbb{Z}$. Nach dem chinesischen Restsatz ist $G \cong \mathbb{Z}/|G|\mathbb{Z}$.

Sei G eine endliche Gruppe, die auf einer endlichen Menge X operiere. Dann muss $|G|$ ein Teiler von $|X|$ sein.

Falsch: Denn für jede Menge X ist $\triangleright: G \times X \to X$, $g \triangleright x = x$ eine Gruppenoperation von G auf X. Wir können zum Beispiel $G = S_3$ und $X = \{*\}$ wählen und es ist $|G| \nmid |X| = 1$.

Es existiert genau ein unitaler Ringhomomorphismus $f: \mathbb{R} \to \mathbb{Z}$.

Falsch: Für einen unitalen Ringhomomorphismus $f: \mathbb{R} \to \mathbb{Z}$ gilt $f(0) = 0$ und $f(1) = 1$. Daraus folgt:

$$2 = f(1) + f(1) = f(2) = f\left((\sqrt{2})^2\right) = f(\sqrt{2})^2 = a^2$$

mit $a := f(\sqrt{2}) \in \mathbb{Z}$. Die Gleichung $a^2 = 2$ hat aber keine Lösung in $\mathbb{Z}$! Also gibt es keinen unitalen Ringhom. $f: \mathbb{R} \to \mathbb{Z}$!

✓ In einer Gruppe ist jedes Element zu seinem Inversen konjugiert.

Falsch: Zum Beispiel ist in abelschen Gruppen jedes Element nur zu sich selbst konjugiert.

✓ Das Bild eines Gruppenhomomorphismus ist immer ein Normalteiler.

Falsch: Zum Beispiel gibt es einen Gruppenhom. $S_4 \to S_3$ und S_3 ist nicht normal in S_4.

✓ Sei R ein kommutativer Ring mit Eins, aber nicht der Nullring. Dann besitzt R ein Primideal.

Wahr: R besitzt laut Vorlesung ein maximales Ideal. Dieses ist prim.

✓ Für alle $a, n \in \mathbb{Z}$ gilt $a^{n-1} \equiv 1 \bmod n$.

Falsch: $6^2 = 36 \equiv 0 \bmod 3$ (Gilt nur für Primzahlen).

Im endlichen Körper $\mathbb{F}_{10^9}$ besitzt jedes Element eine dritte Wurzel.

Wahr: Die Abbildung $\mathbb{F}_{10^9}^* \to \mathbb{F}_{10^9}^*$, $x \mapsto x^3$ ist ein Homomorphismus mit Kern der Ordnung ≤ 3. Da 3 aber kein Teiler von 10^9 ist, muss der Kern trivial sein. Damit ist die Abbildung injektiv und somit bijektiv.

✓ Sei $\phi: G \to H$ ein Gruppenhom. und N ein Normalteiler von G. Dann ist $\phi(N)$ ein Normalteiler von $\phi(G)$.

Wahr: Der Hom. $G \to \phi(H)$ ist surjektiv. Damit folgt die Behauptung.

✓ In der symmetrischen Gruppe S_n ist jede Permutation zu ihrer Inversen konjugiert.

Wahr: Das Inverse eines Elements hat den gleichen Zykel-Typ und alle Zykel dieses Typs liegen in der gleichen Konjugationsklasse.

✓ Jeder kommutative Ring ist isomorph zu einem Teilring eines Körpers.

Falsch: Zum Beispiel ist $\mathbb{Z}_6$ ein komm. Ring, hat aber Nullteiler, z.B. $2 \cdot 3 = 6 = 0$. Wenn es einen Iso. ϕ mit einem Teilring eines Körpers gäbe, so wäre $\phi(2)\phi(3) = \phi(2 \cdot 3) = \phi(0) = 0$, was aber in einem Körper nur dann möglich ist, falls $\phi(2)$ oder $\phi(3)$ Null ist. Dann wäre ϕ nicht mehr injektiv.

✓ Seien I und J zwei Ideale eines Rings R. Dann ist ihre Vereinigung ebenfalls ein Ideal.

Falsch: Sei $R = \mathbb{Z}$, dann sind (2) und (3) Ideale, die Vereinigung enthält dann natürlich $2, 3$ aber nicht deren Summe 5.

Sei p eine Primzahl, sodass -2 kein quadratischer Rest mod p ist. Dann ist $2x^2 + 1$ irreduzibel über $\mathbb{F}_p$.

Wahr: Angenommen $f = 2x^2 + 1$ wäre nicht irreduzibel in $\mathbb{F}_p$. Dann hätte f eine Nullstelle $a \in \mathbb{F}_p$. Es gilt also $2a^2 + 1 = 0$ und damit $\left(\frac{1}{a}\right)^2 = -2$. Also wäre -2 doch ein Quadrat in $\mathbb{F}_p$.

Wenn alle Untergruppen $H \neq G$ einer Gruppe G zyklisch sind, so ist auch G zyklisch.

Falsch: $D_3 = \{1, r, r^2, s, sr, sr^2\}$ ist nicht zyklisch und hat jedoch Untergruppen: $\{1\}, \{1, s\} \cong \mathbb{Z}/2\mathbb{Z}$, $\{1, rs\} \cong \mathbb{Z}/2\mathbb{Z}$, $\{1, r^2 s\} \cong \mathbb{Z}/2\mathbb{Z}$, $\{1, r, r^2\} \cong \mathbb{Z}/3\mathbb{Z}$.

Diese sind alle zyklisch.

Wahr oder Falsch?

✓ Seien M und N Normalteiler der Gruppe G. Dann ist auch $M \cap N$ ein Normalteiler der Gruppe G.

Wahr: Sei $x \in M \cap N$ und $g \in G$. Dann ist $g*g^{-1} \in M$ und $g*g^{-1} \in N$ und somit $g*g^{-1} \in M \cap N$, folglich ist $M \cap N \trianglelefteq G$.

✓ Eine Gruppe der Ordnung 16 ist abelsch.

Falsch: D_8 hat 16 Elemente, ist aber nicht abelsch.

✓ Sei $\phi : G \to H$ ein injektiver Gruppenhomomorphismus und sei H kommutativ. Dann ist auch G kommutativ.

Wahr: Wenn ϕ injektiv ist, dann muss $\ker(\phi) = \{e_G\}$ sein und mit dem Homomorphiesatz ist dann $G/\ker(\phi) \cong G \subseteq H$. Somit muss auch G kommutativ sein!

Wenn G, H zyklisch sind, so ist $G \times H$ zyklisch. Wenn $G \times H$ zyklisch ist, sind auch G und H zyklisch.

Wahr: Da G und H zyklisch sind, gibt es ein $g \in G$ und ein $h \in H$ so dass $G = \langle g \rangle$ bzw. $H = \langle h \rangle$. Für jedes $x \in G$ gibt es also ein $a \in \mathbb{N}$ so dass $x = g^a$ und somit $(g,h)^a = (g^a, h^a) = (x, h^a)$. Analog gibt es zu jedem $y \in H$ ein $b \in \mathbb{N}$ so dass $y = h^b$ und somit $(g,h)^b = (g^b, h^b) = (g^b, y)$. Also gibt es zu jedem $(x,y) \in G \times H$ ein $c \in \mathbb{N}$ mit $c := kgV(a,b)$ mit $(x,y) = (g,h)^c = (g^a, g^b)$. Somit wird $G \times H$ von (g,h) erzeugt und ist folglich zyklisch. (Rückrichtung analog)

Für jede a, b in der Gruppe G gilt $o(ab) = o(ba)$.

Wahr: Seien $a, b \in G$ und $n := o(ab)$. Dann ist

$$e = (ab)^n = b(ab)^n b^{-1} = (ba)^n bb^{-1} = (ba)^n$$

- Folglich ist $o(ba) \leq n$. Sei jetzt $m := o(ba)$. Dann ist

$$e = (ba)^m = a(ba)^m a^{-1} = (ab)^m aa^{-1} = (ab)^m,$$

Also ist $o(ab) \leq m$. Da $n = o(ab) \leq m$ und $m = o(ba) \leq n$ ergibt sich $m = n$.

✓ Sei G eine abelsche Gruppe, die Elemente der Ordnung 2 und 3 besitzt. Dann besitzt G auch ein Element der Ordnung 6.

Wahr: Seien $a, b \in G$ mit $o(a) = 2$ und $o(b) = 3$. Dann ist $(ab)^6 \overset{G \text{ abelsch}}{=} a^6 b^6 = (a^2)^3 (b^3)^2 = e$. Also hat ab Ordnung 6.

✓ Es gibt eine Permutation $\alpha \in S_{12}$ mit $\alpha^{13} = id$.

Falsch: Neben der trivialen Lösung $\alpha = id$ gibt es keine weiteren Lösungen. Denn wegen $|S_{12}| = 12!$ gibt es in S_{12} nur Elemente der Ordnung $\{1, 2, 3, \ldots, 12\}$ und 13 ~~hat~~ teilt keine dieser Ordnungen.

✓ Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und N ein Normalteiler von G. Dann ist $H \cap N$ ein Normalteiler von H.

Wahr: Sei $x \in H \cap N$ und $h \in H$. Dann ist $hxh^{-1} \in N$, da N normal in G ist und somit auch in $H \subset G$. Außerdem ist $hxh^{-1} \in H$, da $h \in H$ und $x \in H$. Also ist $hxh^{-1} \in H \cap N$. Somit ist $H \cap N \trianglelefteq H$.

Sei G eine endliche abelsche Gruppe und $H \subseteq G$ eine Untergruppe mit $[G:H] = 5$, dann besitzt G ein Element der Ordnung 5.

Wahr: G endlich, H Untergruppe $\Rightarrow$ Lagrange: $[G:H] = \frac{|G|}{|H|} = 5$ teilt also $|G|$ und da 5 eine Primzahl ist, gibt es ein $x \in G$ mit $o(x) = 5$.

Es gibt einen surjektiven Homomorphismus zwischen der alternierenden Gruppen $A_5 \to A_4$.

Falsch: Sei $\phi : A_5 \to A_4$ ein Homomorphismus. Wir wissen, dass jeder Homomorphismus Elemente der Ordnung n auf Elemente abbildet, deren Ordnung n teilt, d.h. $o(\phi(x)) \mid o(x)$. Weil $|A_5| = \frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$ und $|A_4| = \frac{4!}{2} = 12 = 2^2 \cdot 3$, muss für ϕ folgendes gelten:

- Elemente der Ordnung 5, also alle 5-Zykel aus A_5, werden auf id abgebildet, da nur id als einziges Element aus A_4 die Ordnung 5 teilt. Also $\tau_i \mapsto id$, wobei τ_i ein beliebiger 5-Zykel aus A_5 ist.
- Elemente der Ordnung 3, also alle 3-Zykel aus A_5, werden auf Elemente der Ordnung 3 oder auf id abgebildet.
- Elemente der Ordnung 2, also alle 2-Zykel aus A_5, werden auf Elemente der Ordnung 2 oder auf id abgebildet.
- id wird auf id abgebildet.

Betrachte wir jetzt $\tau, \sigma \in A_5$ mit $\tau := (12)(34)$ und $\sigma := (12345)$. Dann ist

$$\tau \circ \sigma = (12)(34) \circ (12345) = (135).$$

Es gilt:

$$o(\phi(\tau \circ \sigma)) = o(\phi(123)) = 3.$$

Da ϕ ein Homomorphismus ist, gilt andererseits

$$o(\phi(\tau \circ \sigma)) = o(\phi(\tau) \circ \phi(\sigma)) = o(\phi(\tau) \circ id) = o(\phi(\tau)) = 2 \neq 3.$$

Dies ist offenbar ein Widerspruch, es kann also keinen solchen Homomorphismus geben.

G ist eine endliche Gruppe genau dann, wenn $Aut(G)$ eine endliche Gruppe ist. ✓

Falsch: Automorphismen bilden Erzeuger auf Erzeuger ab. Betrachte wir also $G = \mathbb{Z}$. Dann ist $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Also ist $Aut(\mathbb{Z}) = \{1 \mapsto 1, 1 \mapsto -1\}$ und somit endlich. Aber $|\mathbb{Z}| = \infty$.

Es seien G_1, G_2 Gruppen. Wenn $H \leq G_1 \times G_2$ eine Untergruppe ist, ist $H = H_1 \times H_2$ wobei $H_1 \leq G_1$, $H_2 \leq G_2$ Untergruppen sind. ✓

Wahr: Offensichtlich ist $H = H_1 \times H_2 \subset G_1 \times G_2$. Wir müssen also zeigen, dass H_1 bzw. H_2 Untergruppen von G_1 bzw. G_2 sind. Seien $a_1, b_1 \in H_1$ und $a_2, b_2 \in H_2$. Dann ist $(a_1 \cdot b_1, a_2) \in H$ somit $a_1 \cdot b_1 \in H_1$. Analog ist auch $(a_1, a_2 \cdot b_2) \in H$ und somit $a_2 \cdot b_2 \in H_2$. Außerdem ist wegen $(e, e) \in H$ auch $e \in H_1$ und $e \in H_2$. Liegen $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}) \in H$ ist auch $a_1 \in H_1$ und $a_2 \in H_2$. Damit sind für H_1 und H_2 alle UG-Kriterien erfüllt.

Jede Untergruppe der Ordnung 2 ist ein Normalteiler.

Falsch: D_4 hat Untergruppe $U := \{1, s\}$ mit $|U| = 2$. Angenommen U wäre Normalteiler von D_4, dann müsste $dud^{-1} \in U$ für alle $d \in D_4$ und $u \in U$ gelten. Allerdings ist $rsr^{-1} = r^2 s \notin U$. Also ist U auch nicht normal in D_4.

Wenn die Ordnung einer endlich abelschen Gruppe nicht durch eine Quadratzahl teilbar ist, muss die Gruppe zyklisch sein. ✓

Falsch: S_3 ist bekanntlich nicht abelsch und somit auch nicht zyklisch. Außerdem ist $|S_3| = 3! = 6$. Alle Teiler von 6 sind 1, 2, 3 und 6. Also gibt es keine Quadratzahl ungleich 1, die $|S_3|$ teilt.

Ein Normalteiler ist Vereinigung von Konjugationsklassen. ✓

Wahr: Sei $N \trianglelefteq G$. Dann gilt offenbar: $N \supseteq \bigcup_{n \in N} C_G(n)$. Sei jetzt $n \in N$ beliebig. Dann ist $gng^{-1} \in N$ und somit $C_G(n) \in N$. Wegen $ene^{-1} = n$ ist n zu sich selber konjugiert, d.h. $n \in C_G(n)$. Somit $N \subseteq \bigcup_{n \in N} C_G(n)$. Damit folgt die Behauptung $N = \bigcup_{n \in N} C_G(n)$.

Sei eine Gruppe G mit Untergruppen H, U. Wenn $U \trianglelefteq H$ und $H \trianglelefteq G$ ist $U \trianglelefteq G$.

Falsch: Bekanntlich ist $\{1, s\} \trianglelefteq V_4 \trianglelefteq D_4$. Allerdings ist $rsr^{-1} = r^2 s \notin \{1, s\}$. Also ist $\{1, s\}$ nicht normal in D_4. Kleinste Viergruppe $\{1, s, d^2 s, d^2\}$ oder $\{1, r, r^2 s, r^3\}$.

Sei $a, b \in G$ mit $ggT(o(a), o(b)) = 1$. Dann ist $o(ab) = o(a) \cdot o(b)$. ✓

Falsch: In D_2 ist $o(r) = 3$, $o(s) = 2$ und $o(rs) = 2 \neq o(r) \cdot o(s) = 6$.

Der Ring $\mathbb{Q}[x]/(x^2)$ ist nicht euklidisch. ✓

Wahr: (x^2) ist kein Primideal, denn $x \cdot x \in (x^2)$ aber $x \notin (x^2)$. Also ist $\mathbb{Q}[x]/(x^2)$ kein Integritätsbereich und damit nicht euklidisch.

Jede Zahl $n \in \mathbb{N}_{>0}$ mit $n \equiv 1 \bmod 4$ ist in $\mathbb{N}$ Summe von zwei Quadraten.

Falsch: Betrachte $n = 21 \in \mathbb{N}_{>0}$ mit $21 \equiv 1 \bmod 4$. Da $7 \equiv -1 \bmod 4$ ein Teiler von 21 ist mit $7 \cdot 3 = 21$, jedoch 3 ungerade ist, ist 7 kein Teiler mit gerade Vielfachheit. ↯ Satz von Fermat.

Wahr oder Falsch?

Sei $f: R \to S$ ein surjektiver Ringhomomorphismus und sei m ein maximales Ideal von S. Dann ist auch $f^{-1}(m)$ ein maximales Ideal in R.
Falsch: Betrachte $f: \mathbb{Z} \to \mathbb{Q}$ mit $f: x \mapsto x$. Offenbar ist $\{0\}$ ein maximales Ideal von $\mathbb{Q}$ aber z.B. $(2) \subset \mathbb{Z}$ ist maximales Ideal in $\mathbb{Z}$, das $f^{-1}(\{0\})$ als echte Teilmenge enthält.

Wenn R und S Integritätsbereiche sind, so ist auch $R \times S$ ein Integritätsbereich. ✓
Falsch: Betrachte $\mathbb{Z} \times \mathbb{Z}$. Offenbar ist $\mathbb{Z}$ ein Integritätsbereich. Seien jetzt $(1,0), (0,1) \in \mathbb{Z} \times \mathbb{Z}$, dann ist $(1,0)(0,1) = (0,0)$ und somit ist $\mathbb{Z} \times \mathbb{Z}$ nicht nullteilerfrei und damit kein Integritätsbereich.

~~Sind R und S Integritätsbereiche~~

Seien $a, p \in \mathbb{Z}$ mit p prim. Dann ist a genau dann quadratischer Rest mod. p, ✓ wenn $-a$ kein quadratischer Rest mod. p ist.
Falsch: Wähle $a=1$ und $p=5$. Dann ist $\left(\frac{1}{5}\right) = 1$ und $\left(\frac{-1}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = 1$
D.h. $a=1$ ist quadratischer Rest mod. 5, aber $-a = -1$ ist ebenfalls quadratischer Rest mod. 5.

Sei $\mathbb{K}$ ein Körper und seien $f(x), g(x) \in \mathbb{K}[x]$. Wenn $f(x) \in (g(x))$ und $\deg(f) = \deg(g)$, dann ist $(f(x)) = (g(x))$.
Wahr: Sei $f \in (g)$, also $f = gq$ mit $q \in \mathbb{K}[x]$. Dann muss gelten
$\deg(f) = \deg(g \cdot q) = \deg(g) + \deg(q) \overset{!}{=} \deg(g)$.
Folglich ist $\deg(q) = 0$, also ist $q \in \mathbb{K}$ konstant und somit $(f) = (gq) = (g)$.

In euklidischen Ringen ist jedes Primideal ein Hauptideal. ✓
Wahr: Jeder euklidische Ring ist ein Hauptidealring, d.h. jedes Ideal ist Hauptideal.

Seien p, q Primzahlen $(p \neq q)$. Wenn die Kongruenzen $x \equiv a \bmod p$ und $x \equiv a \bmod q$ lösbar sind, hat $x \equiv a \bmod pq$ eine Lösung.
Wahr: Da $x \equiv a \bmod p$ und $x \equiv a \bmod q$ beide lösbar sind, muss $\left(\frac{a}{p}\right) = 1$ und $\left(\frac{a}{q}\right) = 1$ gelten. Folglich gilt: $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1 \cdot 1 = 1$.

Sei $p \neq 5$, $p \neq 2$ eine Primzahl. Dann ist 5 genau dann quadratischer Rest mod p wenn p quadratischer Rest mod 5 ist. ✓
Wahr: Es gilt $\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}} \left(\frac{p}{5}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$.

Das direkte Produkt $\mathbb{R} \times \mathbb{R}$ ist ein zu $\mathbb{C}$ isomorpher Körper. ✓
Wahr: $\phi: \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ mit $\phi: (a,b) \mapsto a + ib$ ist ein Isomorphismus.

Für $a, b \in \mathbb{Z}$, seien die Hauptideale $(a), (b)$. Dann gilt $(a) \cap (b) = (\text{kgV}(a,b))$. ✓
Wahr: Jedes Ideal in $\mathbb{Z}$ hat die Form $a\mathbb{Z}$ mit $a \in \mathbb{Z}$. Also gilt:
$(a) \cap (b) = a\mathbb{Z} \cap b\mathbb{Z} = \{x \in \mathbb{Z} \mid a \mid x, b \mid x\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}: x = kab\}$
$= \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}: x = k \cdot \text{kgV}(a,b)\} = (\text{kgV}(a,b))$.

Sei $\phi: R \to S$ ein Ringhomomorphismus. Dann ist $\phi(R)$ ein Ideal von S.
Falsch: Seien R, S unitäre Ringe. Angenommen $1 = \text{im}(f)$ wäre ein Ideal in S. Dann müsste das Einselement im Ideal I enthalten sein. Folglich müsste $I = S$ gelten und somit müsste f surjektiv sein. Für Ringhomomorphismen, die nicht surjektiv sind, ist die Behauptung falsch.

$\mathbb{Z}[x]$ ist ein Hauptidealring. ✓
Falsch: $(2, x)$ ist maximal in $\mathbb{Z}[x]$. Allgemein ist (p, x) maximal in $\mathbb{Z}[x]$.

Für $a, b \in \mathbb{Z}$, gilt $(a,b) = (\text{ggT}(a,b))$, ($(a,b)$ ist das Ideal, das von x erzeugt ist). ✓
Wahr: Es ist $(a,b) = a\mathbb{Z} + b\mathbb{Z}$. Also hat $u \in (a,b)$ die Form $ax + by$ mit $x, y \in \mathbb{Z}$. Seien jetzt $g := \text{ggT}(a,b)$ und $a', b' \in \mathbb{Z}$ so dass $a = a'g$ und $b = b'g$. Dann gilt
$ax + by = a'gx + b'gy = g(a'x + b'y) \in g\mathbb{Z} = (g)$.
Umgekehrt können wir die Definition des ggT auch $g = ax + by$ für gewisse $x, y \in \mathbb{Z}$ schreiben. Also ist auch $(g) \in (a,b)$. Somit gilt die Gleichung $(a,b) = (g)$.

Sei $\phi: R \to S$ ein Ringhomomorphismus und $I \subseteq S$ ein Ideal. Dann ist $\phi^{-1}(I)$ ein Ideal von R.
Wahr: Es gilt $\phi^{-1}(I) = \{r \in R \mid \phi(r) \in I\} := J$. Weil I eine Untergruppe von S ist, ist J eine Untergruppe von R. Und für ein Element $r \in R$ und $j \in J$ ist auch $rj \in J$, denn $\phi(rj) = \phi(r)\phi(j) \in I$ (da $\phi(j) \in I$) liegt. Damit ist J Ideal von R.

Für jede Primzahl p ist $\mathbb{F}_p[x]$ ein Hauptidealring.
Wahr: $\mathbb{F}_p$ ist Körper, damit euklidisch, damit ein Hauptidealring.

Für $n \geq 3$ ist $\phi(n) \in 2\mathbb{N}$.
Wahr: Sei $n \geq 3$ mit Primzahlzerlegung

$$n = 2^{\nu_2} \cdot \prod_{p \neq 2 \text{ prim}} p^{\nu_p}$$

Für den Fall $\nu_2 \geq 2$ ist
$$\varphi(2^{\nu_2}) = (2-1)2^{\nu_2 - 1} \in 2\mathbb{Z}.$$
Für $\nu_2 \in \{0,1\}$ gibt es mindestens eine ungerade Zahl p in der Primfaktorzerlegung d.h. $\varphi(p^{\nu_p}) = (p-1)p^{\nu_p - 1} \in 2\mathbb{Z}$.
Folglich hat $\varphi(n)$ mindestens einen gerade Faktor und somit ist $\varphi \in 2\mathbb{Z}$.

Für alle $n \in \mathbb{N}$ gilt $\phi(n) \mid n$.
Falsch: Betrachte $n=3 \Rightarrow \varphi(3) = (3-1)3^0 = 2$ aber $2 \nmid 3$.

Jede Zahl $n \in \mathbb{N}_{>0}$ mit $n \equiv 1 \bmod 4$ ist in $\mathbb{N}$ Summe von zwei Quadraten.
Falsch: Betrachte $n = 21 \in \mathbb{N}_{>0}$ mit $21 \equiv 1 \bmod 4$. Da $7 \equiv -1 \bmod 4$ ein Teiler von 21 ist mit $3 \cdot 7 = 21$, jedoch 3 ungerade ist, ist 7 kein Teiler mit gerade Vielfachheit. $\lightning$ zum Satz von Fermat.

Sei $p \neq 5$, $p \neq 2$ eine Primzahl. Dann ist 5 genau dann quadratischer Rest mod. p, wenn p quadratischer Rest mod 5 ist.
Wahr: Es gilt $\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$.

Seien $a, p \in \mathbb{Z}$ mit p prim. Dann ist a genau dann quadratischer Rest mod p, wenn $-a$ kein quadratischer Rest mod. p ist.
Falsch: Wähle $a=1$, $p=5$. Dann ist $\left(\frac{1}{5}\right) = 1$ und $\left(\frac{-1}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = 1$. D.h. $a=1$ ist quadratischer Rest mod 5 aber $-a = 1$ ist ebenfalls quadratischer Rest mod. 5.

Zusätzliche Sätze

Satz: Rationale Nullstellen haben die Gestalt $\frac{s}{r}$ wobei $s \mid a_0$ und $r \mid$ Leitkoeffizient.

Satz: Sei $p \in \mathbb{N}$ eine Primzahl. Dann sind äquivalent:
1) p ist nicht prim in $\mathbb{Z}[i]$
2) $p = a^2 + b^2$ für $a, b \in \mathbb{Z}$
3) $p = 2$ oder $p \equiv 1 \bmod 4$
4) Das Polynom $x^2 + 1$ ist reduzibel in $\mathbb{F}_p[x]$ (hat also Nullstelle in $\mathbb{F}_p$)
5) -1 ist quadratischer Rest mod. p: $\left(\frac{-1}{p}\right) = 1$

Es gibt einen endlichen Integritätsbereich R, dessen Quotientenkörper $Q(R)$ genau $2 \cdot |R|$ Elemente hat.
Falsch: Jeder endliche Integritätsbereich ist ein Körper, also gilt $R \cong \mathrm{Quot}(R)$ und damit auch $|R| = |\mathrm{Quot}(R)| \neq 2 \cdot |R|$.

Die Zahl $-5 \in \mathbb{Z}[i]$ ist ein Primelement im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen.
Falsch: Denn es gilt $-5 = (2+i)(2-i) = -4^2 - 1^2$ und $2 \pm i \notin \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
Damit ist 5 nicht irreduzibel, aber in jedem Integritätsbereich sind Primelemente irreduzibel.
Alternativ: Laut Vorlesung ist eine Primzahl $p \in \mathbb{N}$ mit $p \equiv 1 \bmod 4$ nicht prim in $\mathbb{Z}[i]$.
Damit ist 5 nicht prim in $\mathbb{Z}[i]$ und damit auch nicht das zu 5 assoziierte Element -5.