Korrekturen und Ergänzungen zum Buch Elementare Algebra und Zahlentheorie, Springer-Verlag, 2. Auflage 2008.

Stand: 3. Mai 2012

Seite 12	Zeile 6	Hat man zwei derartige Darstellungen $f = \prod_{i=1}^{r}(X-\beta_i)^{e_i} g = \prod_{i=1}^{r}(X-\beta_i)^{e_i'} g'$ und ist etwa $e_1 \geq e_1'$, so kann man, da $K[X]$ nullteilerfrei ist,
Seite 27	Zeile 5	Aussage b) ergibt sich unmittelbar aus der Definition einer Primzahl durch die Eigenschaft der Unzerlegbarkeit.
Seite 35	Zeile 1	Sei $n \in \mathbb{N}$ keine Primzahl, $n > 1$, sei $p(n)$ der kleinste Primteiler von n. Dann gilt $p(n) \leq \lfloor \sqrt{n} \rfloor$.
Seite 44	Zeile 13	Sei $a \notin R^\times, a \neq 0$ mit zwei Zerlegungen $a = p_1 \cdots p_r = q_1 \cdots q_s$ in unzerlegbare Elemente p_i, q_j (die dann nach Schritt 3 auch Primelemente sind) gegeben.
Seite 47	Zeile 17	$a_j = q_j a_{j+1} + a_{j+2} \quad (1 \leq j \leq n-1)$ mit $\nu(a_{j+2}) < \nu(a_{j+1}) \quad (1 \leq j \leq n-2)$
Seite 50	Zeile 7	ist genau dann mit $x_1, \ldots, x_k \in \mathbb{Z}$ lösbar, wenn $\mathrm{ggT}(a_1, \ldots, a_k)$ ein Teiler von c ist.
Seite 61	Zeile 17	Beim ISBN-Code von Büchern wurde bis 2006 einer aus 9 Ziffern
Seite 61	Zeile -2	d) Seit 2007 wurde auf ein neues System mit 13 Ziffern umgestellt (ISBN-13), das mit dem allgemeinen Strichcode für Waren (EAN) kompatibel ist. Dabei wird die dreizehnte Ziffer aus den die eigentliche Information enthaltenden ersten zwölf Ziffern nach der Regel $a_{13} + \sum_{j=1}^{6}(a_{2j-1} + 3a_{2j}) \equiv 0 \bmod 10$ berechnet. Welche Vor- und Nachteile hat das neue System?
Seite 66	Zeile 4	$f(a) \in J$
Seite 71	Zeile -3	$\hat{m}_1 = 35 \equiv -1 \bmod 12$ $\hat{m}_2 = 84 \equiv -1 \bmod 5,$
Seite 95	Zeile -16	Ist $S \subseteq G$ eine Teilmenge der Gruppe G, so heißt $\langle S \rangle := \bigcap_{U \subseteq G \text{ Untergruppe}, U \supseteq S} U$ die von S *erzeugte Untergruppe*.
Seite 111	Zeile 8	Da N von H normalisiert wird.
Seite 124	Zeile 14	$\{(M_1, \ldots, M_r) \in (\mathfrak{P}(\{1, \ldots, n\}))^r$
Seite 126	Zeile -7	b) Ist $\lvert G \rvert = p^k m$ mit $p \nmid m$, so heißt eine Untergruppe $H \leq G$ mit $\lvert H \rvert = p^k$ eine *p-Sylowgruppe (p-Sylow-Untergruppe)* von G.
Seite 127	Zeile 7	$\lvert G \rvert = \lvert Z(G) \rvert + \sum_{s \in R'}(G : Z_G(s))$
Seite 127	Zeile 9	... einem Element ist, insbesondere ...
Seite 139	Zeile 10	Ist etwa V ein $\mathbb{R}$-Vektorraum und $f : V \longrightarrow \mathbb{R}$ eine Linearform auf V, so

Seite 156 Zeile 11
und setzen $M_r := F_r \cap M$, ferner betrachten wir für $1 \leq j \leq n$ die j-te Koordinatenabbildung $\pi_j : R^n \longrightarrow R$ $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_j$.

Seite 162 Zeile 13
Für $\mathrm{ggT}(a,m) = 1$ folgt $a^{\varphi(m)} \equiv 1 \bmod m$ ebenso wie der Spezialfall $a^{p-1} \equiv 1 \bmod p$ daraus, dass $x^{|G|} = e$ in jeder Gruppe G für alle $x \in G$ gilt.

Seite 162 Zeile -5
Will jetzt $P_1 =$ Alice eine Nachricht an $P_2 =$ Bob schicken, so wandelt sie ihre Nachricht zunächst (nach irgendeinem allgemein bekannten und leicht umkehrbaren Verfahren) in Zahlen x um $(x < \min(p_2, q_2))$

Seite 169 Zeile 14
Diese Bedingung ist genau dann erfüllt, wenn $a^{\frac{p-1}{q}} \not\equiv 1 \bmod p$ für alle Primzahlen $q|(p-1)$ gilt und für $\nu > 1$ zusätzlich $a^{p-1} \not\equiv 1 \bmod p^2$ gilt.
Insbesondere ist jede Primitivwurzel modulo p^2 auch für alle $\nu \geq 2$ Primitivwurzel modulo p^ν.

Seite 169 Zeile -9
Dann heißt die Zahl $x \in \mathbb{N}_0$, $0 \leq x < \varphi(p^\nu)$ mit $a^x \equiv b \bmod p^\nu$ der *Index* $\mathrm{ind}_a(b) = \mathrm{ind}_{a,p^\nu}(b)$ von b bezüglich a (modulo p^ν).

Seite 183 Zeile 13
a) Mit Hilfe des quadratischen Reziprozitätsgesetzes lassen sich Legendre-Symbole recht schnell ausrechnen; wir haben zum Beispiel $\left(\frac{3}{107}\right) = -\left(\frac{107}{3}\right) = -\left(\frac{2}{3}\right) = 1$.
Als Übung rechne man eine Reihe ähnlicher selbstgewählter Beispiele.

Seite 199 Zeile -8
Sei
$R_0 := \{n1_R \mid n \in \mathbb{Z}\} \subseteq R$
$K_0 := \{\frac{n1_R}{m1_R} \mid n, m \in \mathbb{Z}, m1_R \neq 0_R\} \subseteq K$.

Seite 210 Zeile 17
Sei K ein Körper, $f, g \in K[X]$.
a) Ist $h = \mathrm{ggT}(f,g)$ in $K[X]$ und L ein Erweiterungskörper von K, so ist $h = \mathrm{ggT}(f,g)$ in $L[X]$.
b) Ist L ein Erweiterungskörper von K, in dem $f = \sum_{j=0}^{n} c_j X^j \in K[X]$ in Linearfaktoren zerfällt, so hat f in L genau dann eine mehrfache Nullstelle, wenn $\mathrm{ggT}(f, f') \neq 1$ ist. Dabei ist $f' = \sum_{j=1}^{n} j c_j X^{j-1}$ die formale Ableitung von f.
c) Ist $f \in K[X]$ irreduzibel und L wie in b), so hat f in L genau dann eine mehrfache Nullstelle, wenn $f' = 0$ ist.

Seite 227	Zeile 14	$q-1 = p^{kd}-1$ $= (p^k-1)(1+p^k+\cdots+p^{(d-1)k})$ $=: (p^k-1)\cdot t$
Seite 227	Zeile 12	und nach d) folgt, dass k ein Teiler von r ist.
Seite 228	Zeile 11	In der linken Hälfte des folgenden Diagramms ist $\mathbb{F}_{64}$ mit seinen Teilkörpern dargestellt
Seite 235	Zeile -2	Ist etwa das Minimalgewicht des Codes $d \geq 2t+1$, so gibt es zu jedem auf der Empfängerseite des Kanals empfangenen Element $\mathbf{x}$ von $\mathbb{F}_q^n$ höchstens ein Element $\mathbf{c}$ des Codes, das sich von $\mathbf{x}$ in nicht mehr als t Stellen unterscheidet
Seite 237	Zeile -12	$\deg(h) = k$
Seite 238	Zeile 11	und ist äquivalent zu dem vom Kontrollpoynom X^3+X^2+1 erzeugten Code.
Seite 244	Zeile 7	Zeigen Sie: Ist $K = \mathbb{F}_q$ mit $q = p^m$, so ist $c^{p^{m-1}}$ für jedes $c \in \mathbb{F}_q$ eine p-te Wurzel aus c.