II

Ringe

2.1. Ein Ring R ist eine Menge mit zwei assoziativen Verknüpfungen, $+$ und $\cdot$, mit den folgenden Eigenschaften:
(1) R ist eine kommutative Gruppe mit der Verknüpfung $+$. Das neutrale Element bzgl. $+$ bezeichnet man mit 0.
(2) Es gelten die Distributivgesetze, also
$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$
$$(a+b) \cdot c = a \cdot c + b \cdot c \quad \text{für alle } a,b,c \in R.$$
$(R,+)$ abelsche Gruppe, $(R,\cdot)$ Halbgruppe + Distributivität
(3) Es gibt ein neutrales Element $1 = 1_R \in R$ bzgl. der Verknüpfung $\cdot$.
R heißt kommutativ, falls $(R,\cdot)$ kommutiert.

Bsp.: (1) $\{0\}$ ist der Nullring und der einzige Ring mit $0=1$.

2.3. Ein Element $a \in R$ heißt invertierbar oder Einheit wenn es ein Element $b \in R$ gibt mit $a \cdot b = b \cdot a = 1$. Die Menge der Einheiten heißt $R^\times$.

Bem. $(R^\times, \cdot)$ ist eine Gruppe.
$(R^\times, +)$ ist nicht unbedingt eine Gruppe. ⚠

2.4. Seien R und S Ringe. Eine Abbildung $\phi: R \to S$ heißt Ringhomomorphismus (unitaler), falls $\phi(1_R) = 1_S$ gilt und ϕ verträglich ist mit den Verknüpfungen auf R und S, wenn also
$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) \quad \text{für alle } a,b \in R.$$
$\ker(\phi) := \{a \in R \mid \phi(a) = 0\}$ ist eine Gruppe.

2.5 Ein Ring R ist ein Schiefkörper, wenn $1 \neq 0$ gilt und alle von Null verschiedenen Elemente Einheiten sind (wenn also $R^\times = R \setminus \{0\}$).
Ein kommutative ~~Kö~~ Schiefkörper heißt Körper.

2.6. Sei R ein Ring.
(1) Ist R kommutativ und $a,b \in R$, so heißt a ein Teiler von b (man sagt auch a teilt b), falls es ein $d \in R$ gibt mit $ad = b$. (Jedes Element teilt die Null.)
$a \mid b$, falls a ein Teiler von b ist.
(2) Ein Element $a \in R$ heißt Nullteiler, falls es ein $b \in R$ gibt mit $b \neq 0$, aber $ab = 0$ oder $ba = 0$.
(3) R heißt nullteilerfrei, falls 0 der einzige Nullteiler ist.
(4) R heißt Integritätsbereich, wenn R kommutativ und nullteilerfrei und nicht der Nullring ist. (Auch Integritätsring genannt)

Bsp.: Sei X eine nicht-leere Menge und R ein Ring. Dann ist $R^X = \{f: X \to R\}$, die Menge aller Abbildungen von X nach R, mit der komponentenweisen Addition und Multiplikation wieder ein Ring. Er ist nullteilerfrei genau dann, wenn X aus einem Element besteht.

Bem.: In Integritätsbereichen kann man „kürzen": ✓
Ist $ab = ac$ und $a \neq 0$, so folgt $b = c$, denn aus $a(b-c) = 0$ folgt $b-c=0$.

2.9. $I \subset R$ heißt Ideal, falls $(I,+) \overset{UG}{\leq} (R,+)$ und $R \cdot I \subset I$ und $I \cdot R \subset I$ gilt.

Bsp.: (1) Der Kern $\phi^{-1}(0)$ eines Ringhom. ist ein Ideal.
(2) Jede UG in $\mathbb{Z}$ ist ein Ideal in $\mathbb{Z}$. ↳ Gestalt $m\mathbb{Z}$

Bem.: Schnitte von Idealen sind Ideale.

Für eine Teilmenge $T \subset R$ definieren wir (T) als $(T) := \bigcap_{\substack{T \subset I \subset R \\ I \text{ Ideal in } R}} I$.
(T) ist das kleinste Ideal, dass T enthält. → Hauptidealring: alle Ideale sind H.I.
Ideale, die von einem Element erzeugt werden heißen Hauptideale.

2.11 Sei $I \subset R$ ein Ideal.
(1) Die Verknüpfung $(a+I)\cdot(b+I) = a\cdot b + I$ definiert auf R/I die Struktur eines Rings.
(2) Die kanonische Abbildung $can: R \to R/I$ ist ein Hom. von Ringen mit $can^{-1}(0) = I$.
(3) Ist $\phi: R \to R'$ ein Ringhom. mit $I \subset \ker(\phi)$, so ist der induzierte Gruppenhom. $\bar{\phi}: R/I \to R'$ ein Ringhom.

Bsp.: $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring für jedes $m \in \mathbb{N}$.

2.2 Primkörper

2.13 $I = \{0\}$ und $I = K$ sind die einzigen Ideale in einem Körper K.

Bem.: Ein kommutativer Ring R, der nicht der Nullring ist, ist genau dann ein Körper, wenn er nur Ideale $\{0\}$ und R hat.
Jeder Ringhom. $\phi: K \to R$ in einen vom Nullring verschiedenen Ring ist injektiv.

2.15 Sei $m \in \mathbb{N}$, $m > 0$. Genau dann ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper, wenn m prim ist. $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

2.16 (Kleiner Fermat) Ist p eine Primzahl und $a \in \mathbb{Z}$, so gilt $a^p \equiv a \mod p$.

2.3 Potenzreihen und Polynomringe

Sei R ein Ring, dann ist $R[[X]]$ der Ring der Potenzreihen mit Koeffizienten in R.
$R[[X]] := \{ f: \mathbb{N} \to R \}$ mit $a+b: \mathbb{N} \to R$, $(a+b)(n) = a(n) + b(n)$
$a\cdot b: \mathbb{N} \to R$, $(a\cdot b)(n) = \sum_{\substack{i,j \in \mathbb{N} \\ i+j=n}} a(i)\cdot b(j)$.

Bem.: $a_0 + a_1 X + a_2 X^2 + \dots \in R[[X]]^\times \iff a_0 \in R^\times$.

Der Ring der Polynome $R[X] \subset R[[X]]$ ist definiert als folgende Menge:
$R[X]: \{ \sum_{i=0} a_i X^i \mid a_i = 0$ für fast alle $i \}$.

Ein Polynom der Form $P(X) = a_0$ heißt konstant.
Ist $\phi: R \to R'$ ein Ringhom. und $x \in R'$ ein Element, das mit jedem Element aus $\phi(R)$ kommutiert, so definiert $ev_x: R[X] \to R'$, $P(X) = \sum_{i=0} a_i X^i \longmapsto P(x) := \sum_{i=0} \phi(a_i) x^i$. Notation: $P(x) = ev_x(P)$.

Bem.: Addition komponentenweise.
Multiplikation
$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{l=0}^{p} c_l X^l \quad \text{mit } p = m+n \text{ und } c_l := \sum_{r=0}^{l} a_r b_{l-r}$$

Anmerkung: $R = \mathbb{F}_p$, p prim
$P(X) = X^p - X \in \mathbb{F}_p[X]$
$\Rightarrow X^p - X = \prod_{a \in \mathbb{F}_p} (X - a) \Rightarrow \eta(X^p - X)$ ist die Nullabbildung

Ist K ein Körper: dann ist $\eta: K[X] \to Abb(K,K)$ injektiv, genau dann wenn K unendlich viele Elemente hat.

2.4 Nullstellen von Polynomen

Sei R ein kommutativer Ring. Dann können wir für jedes Polynom $P(X) = a_0 + a_1 X + \dots + a_n X^n \in R[X]$ und jedes $r \in R$ das Element $P(r) = a_0 + a_1 r + \dots + a_n r^n$ bilden.

2.18 Das Element $r \in R$ ist eine Nullstelle von P, falls $P(r) = 0$.

2.19 Ist K ein Körper mit der Eigenschaft, dass jedes nicht konstante Polynom $P \in K[x]$ eine Nullstelle hat, so heißt K algebraisch abgeschlossen.

Bem.: $\mathbb{C}$ ist algebraisch abgeschlossen.
$\mathbb{R}$ ist nicht algebraisch abgeschlossen. Suche Nullstellen von x^2+1.
!A. $\exists$ für jeden Körper K ein Körper L, so dass $K \subseteq L$ und L algebraisch abg.

2.20 (Zerlegung in Linearfaktoren) Ist K ein algebraisch abgeschlossener Körper und $P \in K[x]$ nicht das Nullpolynom, so gibt es ein eindeutig bestimmtes $c \in K$ und eindeutig bis auf Reihenfolge bestimmte $a_1, \dots, a_n \in K$ mit

$$P(x) = c \cdot (X-a_1) \cdots (X-a_n).$$

2.20 Sei R ein nullteilerfreier Ring. Ist $P(x) = a_0 + a_1 X + \dots + a_n X^n \in R[x]$ und $a_n \neq 0$ so ist grad $P := n$ und a_n der Leitkoeffizient von P.
Der Grad des Nullpolynoms ist $-\infty$.

Polynomdivision
Teilen mit Rest

2.21 $R[x]$ ist ein nullteilerfreier Ring und es gilt grad $P \cdot Q$ = grad P + grad Q für $P, Q \in R[x]$, beide $\neq 0$. ⚠

2.22 Sind $P, Q \in K[x]$ und $Q \neq 0$, so gibt es eindeutig bestimmte Polynome $D, S \in K[x]$ mit grad $S <$ grad Q, so dass $P = D \cdot Q + S$.

2.23 Ist $r \in K$ eine Nullstelle von $P \in K[x]$, so gibt es ein Polynom $D \in K[x]$ mit $P = D \cdot (X - r)$.

2.24 Ist $P \in K[x]$, $P \neq 0$, so ist die Zahl der Nullstellen von P kleiner oder gleich dem Grad von P. $\deg(0(x)) = -\infty$, da das Nullpolynom als einziges Polynom unendlich viele Nullstellen hat.

Bem.: $R[x]$ ist nullteilerfrei, falls R nullteilerfrei ist.

2.5 Primideale und maximale Ideale

Sei R ein kommutativer Ring und $I \subset R$ ein echtes Ideal ($I \neq R$).

2.25 (1) I heißt Primideal, falls aus $a, b \in R$ mit $ab \in I$ folgt, dass $a \in I$ oder $b \in I$.
(2) I heißt maximales Ideal, falls es kein echtes Ideal $J \subset R$ gibt mit $I \subset J \subset R$ und $I \neq J$.

2.26 Ein echtes Ideal $I \subset R$ ist genau dann maximal, wenn R/I ein Körper ist.
Es ist genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.

Bem.: Sei K ein beliebiger Körper, $P \in K[x] \setminus \{0\}$. Dann gibt es höchstens grad P Nullstellen von P.

Bem.: Körper sind Integritätsbereiche, maximale Ideale sind prim.

Bsp.: (1) R Integritätsbereich $\Leftrightarrow$ $(0) = \{0\}$ ist Primideal
$(a, b \in R,\ a \cdot b \in (0)$, also $ab = 0 \Rightarrow a = 0 \vee b = 0$, d.h. $a \in (0) \vee b \in (0))$
(2) $m\mathbb{Z} \subseteq \mathbb{Z}$ Primideal ($m \in \mathbb{Z}$) genau dann, wenn $m = 0$ oder $m = p$ oder $m = -p$ für eine Primzahl p.
$(m = \pm ab,\ a, b > 1 \Rightarrow ab \in m\mathbb{Z},\ a, b \notin m\mathbb{Z})$
(3) $m\mathbb{Z} \subseteq \mathbb{Z}$ maximal $\Leftrightarrow m = p \vee m = -p$ für p prim
($\mathbb{Z}/m\mathbb{Z}$ Körper $\Leftrightarrow m = \pm p$)
$ab\mathbb{Z} \subsetneq a\mathbb{Z} \subseteq \mathbb{Z}$ falls $|b| > 1$.
(4) $(x-a) \subset K[x]$ für $a \in K$ ist maximal, da $K[x]/(x-a) \cong K$.

2.6. Der chinesische Restsatz. Sind $R_1, \dots, R_n$ Ringe, so wird das kartesische Produkt $R_1 \times \dots \times R_n$ mittels komponentenweiser Addition und Multiplikation wieder zu einem Ring.

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$
$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 \cdot b_1, \dots, a_n \cdot b_n).$$

Ist R ein Ring und sind $I, J \subset R$ Ideale in R, so ist die Menge $I + J = \{i + j \mid i \in I, j \in J\}$ wieder ein Ideal. Die Menge $\{i \cdot j \mid i \in I, j \in J\}$ ist i. A. kein Ideal, sogar i. A. keine UG von R.

$I \cdot J := (\{i \cdot j \mid i \in I, j \in J\})$, das von allen Produkten erzeugte Ideal. $I \cdot J = \{\sum_{i=0}^{n} a_i i_i j_i \mid i_i \in I, j_i \in J, a_i \in R\}$

Bem.: Ist R kommutativ, sind I, J Ideale in R mit $I + J = R$, so gilt $I \cdot J = I \cap J$.

2.28 (Der chinesische Restsatz) Sei R ein kommutativer Ring, $I_1, \dots, I_n \subset R$ Ideale in R mit der Eigenschaft $I_r + I_s = R$ für alle Paare (r, s) mit $r \neq s$. So induziert die oben definierte Abbildung φ einen Isomorphismus

$$\varphi : R/(I_1 \cap \dots \cap I_n) \xrightarrow{\sim} R/I_1 \times \dots \times R/I_n$$

2.29 (Anwendung von 2.28: Interpolation durch Polynome)
Ist K ein Körper, $a_1, \dots, a_n \in K$ paarweise verschieden und $b_1, \dots, b_n \in K$, so gibt ~~[illegible]~~ Polynom $P \in K[x]$ mit $P(a_i) = b_i$.

2.7. Irreduzible und prime Elemente

Sei R ein kommutativer Ring mit Eins.

2.30. Ein Element $a \in R$ heißt irreduzibel, wenn es nicht invertierbar ist, und wenn aus einer Darstellung $a = bc$ mit $b, c \in R$ folgt, dass entweder b oder c invertierbar sind.
$\hat{=}$ b oder c sind Einheiten

Bsp.: (1) Ein Element $a \in \mathbb{Z}$ ist genau dann irreduzibel, wenn a oder $-a$ eine Primzahl ist.
(2) Das Polynom $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$ aber reduzibel in $\mathbb{C}[X]$ und $\mathbb{F}_2[X]$.

2.32 Sei R ein Integritätsbereich. Ein Element $p \in R$ heißt prim, falls es nicht Null ist und keine Einheit, und wenn aus $p | ab$ mit $a, b \in R$ folgt $p | a$ oder $p | b$.

Bsp.: Ein Element $a \in \mathbb{Z}$ ist genau dann prim, wenn a oder $-a$ eine Primzahl ist, also genau dann, wenn a irreduzibel ist.

2.34 In einem Integritätsbereich ist ein primes Element irreduzibel.

Bsp.: Irreduzible Elemente müssen nicht prim sein:
In $\mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ ist das Element 2 irreduzibel, aber nicht prim, denn $2 | 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ aber $2 \nmid 1 \pm i\sqrt{5}$.

2.8 Faktorielle Ringe

2.36 Ein Ring R heißt faktoriell, wenn R ein Integritätsbereich ist und $a \in R$, $a \neq 0$ sich als Produkt $a = u p_1 \cdots p_n$ von irreduziblen Elementen $p_1, \dots, p_n \in R$ und einer Einheit $u \in R^*$ schreiben lässt und diese Darstellung eindeutig bis auf Reihenfolge und Einheiten ist.

Bsp. (1) $\mathbb{Z}$ faktoriell (Primfaktorzerlegung)
$6 = 2 \cdot 3 = -(-2) \cdot 3 = (-2) \cdot (-3)$
(2) K Körper $\Rightarrow K[X]$ faktoriell (Beweis folgt später). Gilt nur für Körper

2.38 Ist R faktoriell, so ist jedes irreduzible Element prim.

⚠ Merke: Euklid hat fast immer Recht.
Euklidische Ringe $\subsetneq$ Hauptidealringe $\subsetneq$ faktorielle Ringe $\subsetneq$ Integritätsbereiche $\subsetneq$ Ringe.

2.9. Hauptidealringe

2.39 Ein Integritätsbereich R heißt Hauptidealring, falls jedes Ideal in R ein Hauptideal ist, also von einem Element erzeugt ist. In Formeln: $I \subset R$ ein Ideal, $\exists a \in I$ mit $I = (a)$.

2.40 In einem Hauptidealring ist jedes irreduzible Element prim.

2.10 Euklidische Ringe

2.41 Ein euklidischer Ring ist ein Integritätsbereich R, für den eine Abbildung $d: R\setminus\{0\} \to \mathbb{N}$ existiert mit der Eigenschaft:
$\forall a,b \in R: a \neq 0: \exists q,r \in R: b = qa + r \wedge (r = 0 \vee d(r) < d(a))$.

Bsp.: (1) $\mathbb{Z}$ mit dem Absolutbetrag $|\cdot|$.
(2) Der Polynomring $K[X]$ über einem Körper K mit der Gradabbildung grad.
(3) Der Ring der Gaußschen Zahlen $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ mit der Abbildung $d(a+ib) = a^2 + b^2$.

Bem.: Sei R ein kommutativer Ring, der nicht der Nullring ist. Dann ist R ein Körper genau dann wenn $\{0\}$ und R die einzigen Ideale sind.

Bem.: • $\mathbb{F}_2[X]/(f)$ ist $\mathbb{F}_2$-VR von Dim. $\deg(f)$.
V VR über $\mathbb{F}_q$, $\dim_{\mathbb{F}_q} V = n \Rightarrow |V| = q^n$
$\Rightarrow |\mathbb{F}_2[X]/(f)| = 2^{\deg(f)}$
Ist f irreduzibel von Grad 2, so ist $\mathbb{F}_2[X]/(f)$ ein Körper mit 4 Elementen
• Ist K ein Körper so ist $K[X]$ ein HIR.
• Ist R ein HIR und a irreduzibel $\Rightarrow (a)$ maximal
$I \subsetneq R$ ist maximal, wenn $I \subset J \subsetneq R \Rightarrow I = J$
I maximal $\Leftrightarrow R/I$ ein Körper
$\Rightarrow$ Ist f irreduzibel in $K[X]$, so ist $K[X]/(f)$ ein Körper.
• $K[X]/(f)$ enthält eine Kopie von K, wenn $\deg(f) > 0$.
• $K \subset R \Rightarrow R$ ist ein K-VR

2.43 (1) Jeder euklidische Ring ist ein Hauptidealring
(2) Jeder Hauptidealring ist faktoriell.

2.44 Sei K ein Körper. Dann ist der Polynomring $K[X]$ über K ein euklidischer Ring, also ein Hauptidealring und faktoriell.

2.11 Der Quotientenkörper

Betrachte $X = \{(a,b) \mid a, b \in R, b \neq 0\}$ und auf X die Äquivalenzrelation $(a,b) \sim (a',b')$ genau dann, wenn $ab' = ba'$. Dies ist genau die Forderung. Insbesondere darf man kürzen, also $(ad, bd) \sim (a,b)$ für alle $d \neq 0$.

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$$

2.45 Wir nennen den so aus dem Integritätsbereich R konstruierten Körper $\mathrm{Quot}(R)$ den Quotientenkörper von R.
Die Abbildung can: $R \to \mathrm{Quot}(R)$, $r \mapsto \frac{r}{1}$ ist ein Homomorphismus von Ringen.

2.46 (Die universelle Eigenschaft des Quotientenkörpers). Sei R ein Integritätsbereich und R' ein kommutativer Ring. Sei $\phi: R \to R'$ ein Ringhomomorphismus mit der Eigenschaft, dass $\phi(r) \in R'$ eine Einheit ist für alle $r \neq 0$, also ist $\phi(R \setminus 0) \subset (R')^\times$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\tilde{\phi}: \mathrm{Quot}(R) \to R'$ von Ringen, sodass das Diagramm

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[d, "can"'] & R' \\ \mathrm{Quot}(R) \arrow[ur, "\phi"'] \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd}$$ kommutiert.

Ist K ein Körper, so ist $K[X]/\sim \; = K(X)$.

2.12 Primfaktorzerlegung in Polynomringen

2.48 Sei R ein faktorieller Ring. Dann heißt ein Polynom $P(X) = a_0 + a_1X + \dots + a_nX^n \in R[X]$ <u>primitiv</u> wenn es kein irreduzibles Element $b \in R$ gibt, das alle a_i teilt, wenn es also kein $b \in R$ gibt mit $b \mid P(X)$.

2.49 (Lemma von Gauss) Ist R faktoriell und $P, Q \in R[X]$ primitiv, so ist auch $P \cdot Q \in R[X]$ primitiv. Auch interessant: $G(X) = P(X) \cdot Q(X)$ und $G(X)$ reduzibel in $R[X] = \mathbb{Z}[X] \Rightarrow \exists r, s \in \mathbb{Q}\setminus\{0\}: rP(X), sQ(X) \in \mathbb{Z}[X]$ und $G(X) = rP(X) \cdot sQ(X)$. $\Rightarrow rs = 1$.

2.50 In einem Integritätsbereich R ist ein Element p genau dann prim, wenn $R/(p)$ ebenfalls ein Integritätsbereich ist.

2.51 Der Polynomring $R[X]$ über einem faktoriellen Ring R ist wieder faktoriell.

<u>Bem.</u> Insbesondere sind also die Ringe $\mathbb{Z}[X_1, \dots, X_n]$ und $K[X_1, \dots, X_n]$ faktoriell.

<u>Bem.</u> Ein nicht-konstantes Polynom Q ~~[illegible]~~ $\in R[X]$ ist irreduzibel genau dann, wenn es primitiv und in $\mathrm{Quot}(R)[X]$ irreduzibel ist.

2.52 <u>Ist R ein faktorieller Ring, so ist $P \in R[X]$ genau dann irreduzibel, wenn entweder</u>
<u>(1) P ein konstantes Polynom und irreduzibel als Element in R ist, oder</u>
<u>(2) P ein primitives Polynom und irreduzibel in $\mathrm{Quot}(R)[X]$ ist.</u>

2.13 Das Eisensteinkriterium

2.53 (Eisensteinkriterium) Ist $P(X) = a_nX^n + \dots + a_1X + a_0 \in \mathbb{Z}[X]$ und ist p eine Primzahl mit $p \nmid a_n$, $p \mid a_{n-1}, \dots, p \mid a_0$ und $p^2 \nmid a_0$, dann ist P irreduzibel in $\mathbb{Q}[X]$.

<u>Bem.:</u> Die natürliche Abbildung $\mathbb{Z}[X] \to \mathbb{F}_p[X]$; $F \mapsto \bar{F}$, ist induziert von der natürlichen Abbildung $\mathbb{Z} \to \mathbb{F}_p$. Man nennt diese erste das <u>Reduzieren modulo p</u>.

Hat Polynom keine Nullstelle in kleinem Körper, so auch nicht in größerem Ring.

2.14 Kreisteilungspolynome

2.54 Sei $n \in \mathbb{N}$. Ein $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$ heißt komplexe n-te Einheitswurzel.
Eine n-te Einheitswurzel ist nichts anderes als eine Nullstelle des Polynoms $X^n - 1 \in \mathbb{C}[X]$.

<u>Bem.:</u> (1) Das Produkt zweier Einheitswurzeln ist eine Einheitswurzel.
(2) Das multiplikative Inverse einer n-ten Einheitswurzel ist eine n-te Einheitswurzel.
(3) Die n-ten Einheitswurzeln bilden eine Untergruppe $(\mathbb{C}^\times, \cdot)$.

<u>Bem.:</u> n-te Einheitswurzeln: $(\{e^{\frac{2\pi i k}{n}} \mid k = 0, \dots, n-1\}, \cdot) \cong (\mathbb{Z}/n\mathbb{Z}, +)$.
$(\{e^{\frac{2\pi i k}{n}} \mid k = 0, \dots, n-1\}, \cdot)$ ist zyklisch.

(1) $X^n - 1 = \prod_{\zeta^n = 1} (X - \zeta) = \prod_{k=1}^{n} (X - e^{\frac{2\pi i k}{n}})$, sei für $d \geq 1$: $\phi_d(X) = \prod_{\mathrm{ord}\,\zeta = d} (X - \zeta)$

$\Rightarrow X^n - 1 = \prod_{d \mid n} \phi_d(X)$

<u>Bsp.:</u> (1) $\phi_1(X) = X - 1$, $\phi_2(X) = X + 1$, $\phi_3(X) = (X - e^{\frac{2\pi i}{3}})(X - e^{\frac{2\pi i \cdot 2}{3}})$
$= X^2 - (e^{\frac{2\pi i}{3}} + e^{\frac{2\pi i \cdot 2}{3}})$

Aus $X^3-1 = \Phi_1(x)\Phi_3(x) = (x-1)(x^2-(e^{\frac{2\pi i}{3}}+e^{\frac{2\pi i 2}{3}})x+1)$ erhalten wir $e^{\frac{2\pi i}{3}}+e^{\frac{2\pi i 2}{3}} = 1$, also $\Phi_3(x) = x^2+x+1$.
Ist $n=4$ und $\zeta_1 = i$ und $\zeta_3 = -i$ die einzigen Einheitswurzeln der Ordnung 4 und $\zeta_2 = -1$ die einzige Einheitswurzel der Ordnung 2.
$\Rightarrow \Phi_4(x) = (x+i)(x+1) = x^2+1$ und $\Phi_2(x) = x+1$
$\Rightarrow x^4-1 = \Phi_4\Phi_2\Phi_1 = (x^2+1)(x+1)(x-1)$

Allgemein gilt $X^n-1 = (X-1)(X^{n-1}+X^{n-2}+\dots+1)$ und damit $\Phi_p(x) = X^{p-1}+X^{p-2}+\dots+1$ für eine Primzahl p. Insbesondere $\Phi_p \in \mathbb{Z}[X]$.

2.57 Für alle $d \geq 1$ hat Φ_d ganze Koeffizienten: $\Phi_d \in \mathbb{Z}[x]$.

2.58 Sei p eine Primzahl. Dann ist das p-te Kreisteilungspolynom $\Phi_p \in \mathbb{Q}[x]$ irreduzibel.

Alle Φ_n für $n \geq 1$ sind irreduzibel.

4.1 Der algebraische Abschluss

Bsp. $\mathbb{Z}[x]$ ist nicht euklidisch, kein Hauptidealring
$\mathbb{Z}[x]$, $K[X_1, \dots, X_n]$ sind faktorielle Ringe.

Merke:
Euklidische Ringe
$\cap$
Hauptidealringe
$\cap$
faktorielle Ringe
$\cap$
Integritätsbereiche
$\cap$
Ringe

Primitive Polynome: Für $R = \mathbb{Z}$, $p(x) = 3x+7x^4$ primitiv
$p(x) = 2x+4x^2$ nicht primitiv

Jeder Körper lässt sich in einen algebraisch abgeschlossenen Körper einbetten.
Ein Körper K heißt algebraisch abgeschlossen, falls jedes nicht konstante Polynom $P \in K[X]$ eine Nullstelle in K hat.
Dies ist äquivalent dazu, dass jedes Polynom in $K[X]$ über K in Linearfaktoren zerfällt.

4.1. Eine algebraische Erweiterung $K \subset \overline{K}$ mit algebraisch abgeschlossenem $\overline{K}$ heißt algebraischer Abschluss von K.

4.2. Zu jedem Körper K gibt es einen algebraischen Abschluss $K \subset \overline{K}$. Je zwei algebraische Abschlüsse sind isomorph:
Ist $K \subset \overline{K}'$ ein weiterer algebraischer Abschluss, so gibt es einen Isomorphismus $\phi: \overline{K} \to \overline{K}'$ mit $\phi|_K = \mathrm{id}_K$.

Partielle Ordnung: Sei X eine Menge, so ist eine partielle Ordnung auf X eine Relation $\leq \subset X \times X$ mit den Eigenschaften
(1) $x \leq x$ für alle $x \in X$
(2) aus $x \leq y$ und $y \leq x$ folgt $x = y$ für alle $x, y \in X$
(3) aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ für alle $x, y, z \in X$.
Gilt für alle $x, y \in X$ entweder $x \leq y$ oder $y \leq x$, so nennt man $\leq$ totale Ordnung, $<$.

Bsp. Die natürlichen Zahlen ≥ 1 sind partiell. $(\mathbb{N}, \leq)$ aber nicht total geordnet.

Ist $(X, \leq)$ eine partiell geordnete Menge und $Y \subset X$ eine Teilmenge, so heißt $x \in X$ eine obere Schranke für Y, falls $y \leq x$ für alle $y \in Y$.

Ein Element $x \in X$ mit $x \leq y$ für $y \in X \Rightarrow x = y$, so heißt x maximales Element in X.

4.4 (Lemma von Zorn) Ist $(X, \leq)$ eine partiell geordnete Menge, so dass jede total geordnete Teilmenge $Y \subset X$ eine obere Schranke besitzt, so gibt es in X mindestens ein maximales Element.

Zornsches Lemma:
Jede surjektive Abbildung zwischen zwei Mengen besitzt ein Rechtsinverses.

Bem.: Das Lemma von Zorn und das Auswahlaxiom sind äquivalent.

4.2. Endliche Untergruppen der Drehgruppe.

Sei $SO(3) \subset GL(\mathbb{R}^3)$ die Drehgruppe des euklidischen Raums $\mathbb{R}^3$. Ist $A \subset \mathbb{R}^3$ eine Teilmenge, so nennen wir $g \in SO(3)$ eine Symmetrie von A, falls $g \cdot A = A$ gilt.

4.5 Jede endliche Untergruppe der Drehgruppe $SO(3)$ ist genau eine der folgenden Gruppen:
(1) Eine zyklische Gruppe der Ordnung $n \geq 1$, bestehend aus allen Drehungen um eine feste Achse um den Winkel $2\pi k/n$.
(2) Die Symmetriegruppe eines ebenen gleichseitigen n-Ecks für $n > 2$ oder die Gruppe aller Elemente, die zwei orthogonale Geraden durch den Nullpunkt jeweils in sich überführen (Fall $n=2$). Dies sind die Diedergruppen mit Ordnung $2n$.
(3) Die Tetraedergruppe aller Symmetrien eines Tetraeders (12 Elemente)
(4) Die Würfelgruppe aller Symmetrien eines Würfels (24 Elemente).
(5) Die Ikosaedergruppe (60 Flächen) aller Symmetrien eines Ikosaeders (60 Elemente).

Der Hauptsatz der Algebra

4.6 Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Anmerkung: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$.
$\mathbb{R} \subset \mathbb{C}$ ist separable Körpererweiterung vom Grad 2.
Jedes Polynom in $\mathbb{C}[x]$ vom Grad 2 zerfällt vollständig über $\mathbb{C}$.
Jedes Polynom aus $\mathbb{R}[x]$ von ungeradem Grad in $\mathbb{R}$ hat eine Nullstelle.

Bem.: Ist $R[x]$ faktoriell, so sind Primelemente gleich den irreduziblen Elementen.
$R[x]/(f)$ ist ein Integritätsbereich, genau dann wenn (f) ein Primideal ist.

Das Jacobi-Symbol

$$\left(\frac{a}{n}\right) = \begin{cases} 1, & \text{wenn } a \text{ ein quadratischer Rest mod } n \text{ ist} \\ -1, & \text{wenn } a \text{ ein quadratischer Nichtrest mod } n \text{ ist} \\ 0, & \text{wenn } n \text{ Teiler von } a \text{ ist.} \end{cases}$$

Hier ist n prim.

Berechnung: $n = p_1^{\nu_1} \cdot p_2^{\nu_2} \cdots p_k^{\nu_k}$ mit $p_1, \dots, p_k$ prim

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\nu_1} \cdots \left(\frac{a}{p_k}\right)^{\nu_k}$$

Achtung! ⚠ q muss auch prim sein!

Quadratisches Reziprozitätsgesetz: $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$.