Algebra und Zahlentheorie Stoffsammlung

Gruppen

- Zu jedem $n \in \mathbb{N}^+$ existiert eine Gruppe mit n Elementen (z.B. $\mathbb{Z}/n\mathbb{Z}$)
- Jede abelsche Gruppe ist isomorph zu $\prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$
- $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ wenn a, b teilerfremd
- Sei $p \in \mathbb{N}$ prim, $|G| = p \Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$
- $h \in gU \Leftrightarrow g^{-1}h \in U \Leftrightarrow hU = gU$
- $\forall h, g \in G : |hU| = |gU|$
- $|G| = |U| \cdot (G : U) \qquad (G : U) := |\{gU \mid g \in G\}|$
- $. : G \times \Omega \to \Omega$ Gruppenoperation
  $G_\omega := \{g \in G \mid \omega.g = \omega\} \qquad \omega^G := \{\omega.g \mid g \in G\}$
  Dann gilt: $\left|\omega^G\right| = (G : G_\omega) \qquad \omega^G \to G : G_\omega$ bijektiv
- $|\Omega| = \sum_{i \in I}(G : G_{\omega_i})$ mit $\{\omega_i\}$ Vertreter der Bahnen
- $Z(G) = \left\{\omega \in G \mid \forall g \in G : g^{-1}\omega g = \omega\right\}$ Zentrum von G (Untergruppe)
- $|G| = p^2$ für p prim $\Rightarrow Z(G) = G \Rightarrow G$ ist abelsch
- *Satz von Lagrange:* G endliche Gruppe, $H \subset G$ Untergruppe:

$$|G| = |H| \cdot |G/H| = |H| \cdot |G \backslash H|$$

- N Normalteiler $\Leftrightarrow G/N = G\backslash N$
- G heißt zyklisch, wenn gilt $\exists g \in G : G = \langle g \rangle$
- *Universelle Eigenschaft der Restklassengruppe:*
  1. $can : G \to G/N, g \mapsto gN$ ist Homomorphismus mit Kern N
  2. Ist $\varphi : G \to G'$ ein Homomorphismus mit $\varphi(N) = 1$, so gibt es genau einen Homomorphismus $\overline{\varphi} : G/N \to G'$ mit $\varphi = \overline{\varphi} \circ can$
- $\forall g \in G : ord(g) = |\langle g \rangle| \qquad G$ endlich $\Rightarrow g^{|G|} = 1$
- G endlich, p prim, $P \subset G$ heißt *p-Sylow* gdw $|P|$ die höchste p-Potenz ist, die $|G|$ teilt
- *Sätze von Sylow:* Sei G endlich, p prim, p^r höchste p-Potenz die $|G|$ teilt
  1. G besitzt p-Sylows
  2. Je zwei p-Sylows sind zueinander konjugiert

3. Jede Untergruppe von G, deren Ordnung eine p-Potenz ist liegt in einer p-Sylow
4. Die Zahl der p-Sylows ist ein Teiler von $|G|/p^r$ und kongruent zu $1(p)$

- Sei $P \subset G$ eine p-Sylow:

$$P \text{ ist Normalteiler } \Leftrightarrow P \text{ ist einzige } p\text{-Sylow in } G$$

- *Satz von Cauchy:* Jeder Primfaktor der Ordnung einer endlichen Gruppe tritt auch als Ordnung eines Elements der Gruppe auf

Ringe

- *Nicht* zwangsläufig Nullteilerfrei $\Rightarrow$ Division nicht immer definiert
- R heißt *Integritätsbereich* gdw $R \neq \{0\}, R$ ist Nullteilerfrei
- *Einheit:* Ein Element mit multiplikativ inversem. Einheiten in R bilden die Gruppe $R^\times$
- $\mathbb{Z}/m\mathbb{Z}$ ist Integritätsbereich, falls m prim oder $m = 0$
- *Charakteristik von R:* Kleinstes m, so dass $\sum_{i=1}^{m} 1_R = 0_R$
- $I \subset R$ heißt *Ideal* gdw I Untergruppe bzgl $+$, $RI \subset I$ und $IR \subset I$
- I heißt *Hauptideal* gdw I Ideal und $\exists i \in I : I = \langle i \rangle$
- $a \in R$ heißt *irreduzibel* gdw $a \notin R^\times$ und $a = bc \Rightarrow b \in R^\times \vee c \in R^\times$
- $a \in R, a \notin R^\times$ heißt *Primelement* gdw $a \neq 0$ und $a \mid bc \Rightarrow a \mid b \vee a \mid c$
- *Hauptidealring* Ein Ring, in dem alle Ideale Hauptideale sind
- R heißt *euklidischer Ring* gdw. Division mit Rest existiert.
- R heißt *faktorieller Ring*, wenn R kommutativer Integritätsbereich und jedes Element aus $R \setminus 0$ bis auf Multiplikation mit Einheiten eindeutig als Produkt von irreduziblen Elementen darstellbar ist.
- Euklidische Ringe $\subset$ Hauptidealringe $\subset$ Faktorielle Ringe $\subset$ Integritätsbereich $\subset$ Ringe
  "Euklid hat fast immer Recht"
- Euklidische Ringe erlauben Euklidischen Algorithmus (Polynomringe sind euklidisch)
- In einem Hauptidealring sind die primitiven Elemente genau die irreduziblen Elemente

- Für den Quotienten eines Hauptidealrings nach einem von Null verschiedenen Ideal gilt:
  Der Quotient ist ein Körper $\Leftrightarrow$ Ein und jeder Erzeuger des Ideals ist ein irreduzibles Element
- R faktoriell $\Rightarrow$ $R[X]$ faktoriell mit den irreduziblen Elementen:
  1. Irreduzible Elemente aus R
  2. Primitive Polynome aus $R[X]$, die irreduzibel sind in (Quot R)$[X]$
- *Eisenstein-Kriterium:* Sei $P(X) = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in \mathbb{Z}$
  $P(X)$ ist irreduzibel in $\mathbb{Q}[X]$, wenn eine Primzahl p existiert, so dass:
  $$p \mid a_i \forall i < n \qquad p^2 \nmid a_0 \qquad p \nmid a_n$$
- Sei R faktoriell. $P \in R[X]$ heißt *primitiv* gdw es kein irreduzibles Element von R gibt, dass alle koeffizienten von P teilt. $P \in$ (Quot R)$[X]$ heißt primitiv, wenn $P \in R[X]$ primitiv.
  Das Produkt primitiver Polynome ist primitiv.
  $\Rightarrow \exists\, \text{cont}^{-1}(P) \in (\text{Quot } R)^\times$:$\text{cont}^{-1}(P) \cdot P$ ist primitiv
  $\text{cont}(PQ)$ =$\text{cont}(P)\text{cont}(Q)$
- $P(X_1, ..., X_n)$ heißt symmetrisch, wenn $P = \sigma P\ \forall \sigma \in S_n$
- $P(X_1, ..., X_n)$ heißt *Homogen* vom Grad d, wenn gilt:
  $$P(X_1, ..., X_n) = \sum_{i=0}^{m} a_i \prod_{j=1}^{n} X_j^{\alpha_{ij}} \Rightarrow \sum_{j=1}^{n} \alpha_{ij} = d\ \forall 1 \leq i \leq m$$

Körper

- Die Charakteristik eines Körpers ist entweder 0 oder prim
- $[K(\alpha) : K]$ =Grad$(Irr(\alpha, K))$
- L/K Körpererweiterung, für $\alpha \in L$ gilt:
  $$\alpha \text{ algebraisch über } K \Leftrightarrow [K(\alpha) : K] < \infty \Leftrightarrow \exists K \subset L' \subset L : \alpha \in L', [L' : K] \leq \infty$$
- $[L : K] = 2 \Leftrightarrow \exists \alpha \in K : L = K(\sqrt{\alpha})$
- $K \subset L \subset M \Rightarrow [M : K] = [M : L] \cdot [L : K]$
- K ist endlicher Körper $\Rightarrow |K|$ ist eine Primzahlpotenz
- Eine endliche Körpererweiterung L/K heißt *normal* gdw sie algebraisch ist und jedes Polynom über K mit Nullstelle in L bereits über L in Linearfaktoren zerfällt
  L/K ist normal gdw L Zerfällungskörper eines Polynoms über K ist

- $K \subset L$ Körper mit $\text{char}(K) = 0$
  $\forall P \in K[X] : P$ irreduzibel $\Rightarrow P$ hat keine mehrfachen Nullstellen
- $P \in K[X], P(\alpha) = 0$
  P ist mehrfache Nullstelle $\Leftrightarrow P'(\alpha) = 0$
- P hat mehrfache Nullstellen in $\text{ZFK}(P) \Leftrightarrow P$ und P' sind nicht teilerfremd
- Ein Polynom heißt *separabel* gdw es keine mehrfachen Nullstellen hat
- Sei $P \in K[X]$ irreduzibel, dann:

  P nicht separabel in $\text{ZFK}(P) \Leftrightarrow P' = 0 \Leftrightarrow \text{char}(K) = p > 0,\ \exists Q \in K[X] : P(X) = Q(X^p)$

- L/K heißt separabel gdw jedes Element von L über K separabel ist
- K heißt *vollkommen* gdw $\text{char}(K) = 0$ oder für $\text{char}(K) = p$ die Abbildung $x \mapsto x^p$ surjektiv auf K ist
  Jeder endliche Körper ist vollkommen
- Jedes irreduzible Polynom über einem vollkommenen Körper ist separabel
  Jede algebraische Erweiterung eines vollkommenen Körpers ist separabel
- L/K ist separabel $\Leftrightarrow L$ wird erzeugt aus K von über K separablen Elementen
- ist L/K endlich und separabel, so gibt es $\alpha \in L$ so dass $L = K(\alpha)$
- $K \subset L \subset M$, M/K normal+separabel
  $\Rightarrow M/L$ normal+separabel, L/K separabel, aber i.A. nicht normal
- $K \subset L \subset M$, M algebraisch über L, L algebraisch über $K \Rightarrow M$ algebraisch über K
- K ist Körper der konstruierbaren Zahlen, d.H. der kleinste Teilkörper von $\mathbb{C}$, so dass $\forall x \in K : \sqrt{x} \in K$
- $x \in K \Leftrightarrow x$ ist algebraisch und $\text{Grad}(x)$ ist eine Zweierpotenz
- Ein regelmäßiges n-Eck ist konstruierbar gdw
  $\exists r \in \mathbb{N} : \varphi(n) = |\{a \mid 1 \leq a \leq n, \text{ggT}(a,n) = 1\}| = 2^r$
- $\varphi(nm) = \varphi(n)\varphi(m) \qquad \varphi(p^r) = p^{r-1}(p-1)$ für p prim
- Das n-te Kreisteilungspolynom hat Grad $\varphi(n)$

Galois-Kram

- L/K heißt Galois, wenn L normal und separabel über K
- $|\text{Gal}(L/K)| \leq [L:K]$, $|\text{Gal}(L/K)| \mid [L:K]$
  L/K Galois $\Leftrightarrow |\text{Gal}(L/K)| = [L:K]$

- q Primzahlpotenz, $r \geq 1$, dann ist $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ eine zyklische Gruppe der Ordnung r, erzeugt vom Frobenius-Homomorphismus:

$$\begin{aligned} \mathbb{F}_{q^r} &\to \mathbb{F}_{q^r} \\ a &\mapsto a^q \end{aligned}$$

- $P \in K[X]$ ein Polynom, L/K der Zerfällungskörper, dann operiert $\mathrm{Gal}(L/K)$ *treu* und *transitiv* auf der Menge der Nullstellen
  treu: Nur e bildet neutral ab
  transitiv: Je zwei Elemente lassen sich mit der Gruppenabbildung ineinander überführen (d.h. es gibt nur eine Bahn)
- ist L/K endliche Galoiserweiterung mit Galois-Gruppe G, so entspricht jeder Untergruppe von G ein Zwischenkörper. Insbesondere entspricht jeder Normalteiler von G einem normalen Zwischenkörper
- Eine Körpererweiterung L/K mit $\mathrm{char}(K) \neq 2$ heißt biquadratisch, wenn $[L:K] = 4$ und $L = K(\sqrt{\alpha}, \sqrt{\beta})$ für geeignete $\alpha, \beta \in K$
  Jede biquadratische Körpererweiterung ist Galois mit Galoisgruppe $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  $\Rightarrow G$ hat 5 Untergruppen, korrespondierend zu $K \subset K(\sqrt{\alpha}), K(\sqrt{\beta}), K(\sqrt{\alpha\beta}) \subset L$
- Kreisteilungspolynome sind alle irreduzibel in $\mathbb{Q}$
- $b_1, b_2 \in \mathbb{Z}$ teilerfremd $\Rightarrow a$ ist quadratisch modulo $b_1 b_2$ gdw a quadratisch modulo b_1 und quadratisch modulo b_2
- Seien $p, q > 2$ prim, dann gilt:
  1. $p \equiv 1(4) \vee q \equiv 1(4) \Rightarrow (\exists r : p \equiv r^2(q) \Leftrightarrow \exists s : q \equiv s^2(p))$
  2. $p \equiv 3(4) \wedge q \equiv 3(4) \Rightarrow (\exists r : p \equiv r^2(q) \Leftrightarrow \neg\exists s : q \equiv s^2(p))$
- *Legendre-Symbol:* p prim, $a \in \mathbb{Z}$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a, \exists r : a \equiv r^2(p) \\ -1 & \text{sonst} \end{cases}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(p) \text{ für } p > 2$$

Sondertutorate

Aufgabe 2 Gruppenhomomorphismenbla:

$\forall k \in \mathbb{Z}/m\mathbb{Z} : mk = 0 = \phi(0) = \phi(mk) = m\phi(k) \Rightarrow n \mid m\phi(k)$
$g = \text{ggT}(n,m), n = gn', m = gm' \qquad n \mid m\phi(k) \Leftrightarrow n' \mid m'\phi(k) \qquad gn' \mid gm'\phi(k)$
$(ggT(n',m') = 1) \Rightarrow n' \mid \phi(k) \Rightarrow$ Für jeden Homomorphismus:$n' \mid \phi(k) \forall k \in \mathbb{Z}/m\mathbb{Z}$
$\phi(k) = k\phi(1) \Rightarrow \phi$ is determined by $\phi(1)$
$\phi(1) =$ Any Element of $\mathbb{Z}/m\mathbb{Z}$ that is divisible by n'
$\Rightarrow \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \left\{x \in \mathbb{Z}/n\mathbb{Z} \mid (n' \mid x)\right\}$
$\Rightarrow |\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})| = g = \text{ggT}(n,m)$

Aufgabe 3 (Bild unter surjektivem Normalteilerbla): $\varphi : G \to H$ surjektiv, $N \subset G$ normal
$gNg^{-1} = N \forall g \in G \Rightarrow \forall h \in H \exists g \in G : h\varphi(N)h^{-1} = \varphi(g)\varphi(N)\varphi(g^{-1}) = \varphi(g^{-1}Ng)$
$= \varphi(N)$
Hätte noch zeigen sollen, dass ne Untergruppe, aber wurde großzügig korrigiert

Aufgabe 4 (4900 als Summe von Quadraten): $4900 = 7^2 \cdot 2^2 \cdot 5^2$, Erinnere $\mathbb{Z}[i]$:
$7 \equiv 3 \text{mod} 4 \Rightarrow 7$ ist prim in $\mathbb{Z}[i] \qquad 5 = 1 \text{mod} 4 \Rightarrow$ reduzibel
$5 = (2+i)(2-i), 2 = (1+i)(1-i) \Rightarrow 4900 = 7^2(1+i)^2(1-i)^2(2+i)^2(2-i)^2$
$2^2 = (2i)(-2i),\ 5^2 = (3+4i)(3-4i),\ 10^2 = (8-6i)(8+6i)$
$\Rightarrow 4900 = 7^2 2^2 5^2 = 7^2 2^2 (3+4i)(3-4i) = 7^2 2^2 (3^2+4^2) = 7^2 10^2 = 7^2(8-6i)(8+6i)$
$= 7^2(8^2+6^2)$

Aufgabe 5: P, Q irreduzibel in $K[X]$, $p =$Grad(P), $q =$Grad(Q), ggT$(p,q) = 1$ Sei β Nullstelle von Q, $[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K]$
$= [K(\alpha,\beta) : K(\beta)][K(\beta) : K]$
$\Rightarrow p, q \mid [K(\alpha,\beta) : K] \Rightarrow$kgV$(p,q) \mid [K(\alpha,\beta) : K] \Rightarrow pq \mid [K(\alpha,\beta) : K]$
$\Rightarrow pq \leq [K(\alpha,\beta) : K]$
$[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K] \leq pq \Rightarrow pq = [K(\alpha,\beta) : K]$
$\Rightarrow [K(\alpha,\beta) : K(\alpha)] = q \Rightarrow Q$ irreduzibel über $K(\alpha)$

Aufgabe 6: $M \supset L$ separabel, $L \supset K$ separabel $\Rightarrow M/K$ separabel
$\Rightarrow \forall \alpha \in L :Irr_K(\alpha)$ hat keine Mehrfachen Nullstellen
Sei $\alpha \in M$,Irr$_L(\alpha)$ hat Koeffizienten $\beta_1, ..., \beta_n \in L$
$\Rightarrow K(\beta_1, ..., \beta_n)$ ist separabel und endlich über K
$K(\alpha, \beta_1, ..., \beta_n)$ ist separabel und endlich über $K(\beta_1, ..., \beta_n)$
oBdA $M = K(\alpha, \beta_1, ..., \beta_n)$, $L = K(\beta_1, ..., \beta_n)$ (weil Endlich nach Satz 3.6.17)
$[L : K] = \left|\text{Ring}^K(L, N)\right| = [L : K]^S$(N ist irgendeine normale Erweiterung von K)
$[M : L] = [M : L]^S$
$\Rightarrow [M : K] = [M : L][L : K] = [M : L]^S[L : K]^S = [M : K]^S \Rightarrow M$ separabel über K

Aufgabe 7: Zwischenkörper von $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$
$[\mathbb{Q}(\zeta_{12}):\mathbb{Q}] = \phi(12) = 4 \Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(weil nicht rotationssymmetrisch, also nicht $\mathbb{Z}/4\mathbb{Z}$)
Untergruppen von $\mathbb{Z}/4\mathbb{Z} = \{e, \sigma, \tau, \sigma\tau\}$:
$(\sigma(\zeta_{12}) = \zeta_{12}^5,\ \tau(i) = -i,\ )$

$$\begin{array}{ccc} \{e\} & \leftrightarrow & \mathbb{Q}(\zeta_{12}) \\ \langle\sigma\rangle & \leftrightarrow & \mathbb{Q}(i) \\ \langle\tau\rangle & \leftrightarrow & \mathbb{Q}(\sqrt{3}) \\ \langle\sigma\tau\rangle & \leftrightarrow & \mathbb{Q}(\zeta_{12}^2) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \leftrightarrow & \mathbb{Q} \end{array}$$

Aufgabe 8: $X^2 - 6$ ZFK= $\mathbb{Q}(\sqrt[6]{6}, \zeta_6)$
$[\mathbb{Q}(\sqrt[6]{6}, \zeta_6) : \mathbb{Q}(\sqrt[6]{6})][\mathbb{Q}(\sqrt[6]{6}) : \mathbb{Q}] = 2 \cdot 6 = 12$
Galoisgruppe: Enthält Konjugation und Rotation (der Wurzeln aus 6) $\Rightarrow$ kommutieren nicht

Zu Aufgabe 6 nochmal:
Satz: L/K Endliche Körpererweiterung, separabel gdw für ein M/L mit M normal über K gilt: $\mathrm{Ring}^K(L, M) = [L : K]$ (Anzahl der Körperhomomorphismen)
oBdA $[M : K] < \infty$ (Sonst sei $\alpha \in M, a_i \in L$ Koeffizienten von $\mathrm{Irr}(\alpha, L)$, betrachte $K \subset K(a_0, ..., a_r) \subset K(a_0, ..., a_r, \alpha)$)
$K \subset L \subset M \subset N$, so dass N normal über K, also $\mathrm{Ring}^K(L, N) = [L : K]$, also $\mathrm{Ring}^K(M, N) = \mathrm{Ring}^K(L, N) \cdot [M : L] = [M : L][L : K] = [M : K] \Rightarrow M/K$ separabel

Blatt 3 Aufgabe 2: $\overline{G} = G/N$ auflösbar, N auflösbar $\Rightarrow G$ auflösbar:
$N = N_r \rhd N_{r-1} \rhd ... \rhd N_0 = 1$, N_i/N_{i-1} abelsch
$G = G_s \rhd G_{s-1} \rhd ... \rhd G_0 = N$
$G_i/G_{i-1} \simeq \overline{G}_i/\overline{G}_{i-1} = (G_i/N)/(G_{i-1}/N)$ (Noetherscher Isomorphiesatz)

Baltt 2 Aufgabe 4: surjektiv:$\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z}$
$\mathbb{Z}$ Kern ist zyklisch: Kern wird erzeugt von $1 + p$ (multiplikativ), u.a. weil $|\ker| = p^{r-1}$
Also: $\langle 1 + p\rangle = \ker \subset (\mathbb{Z}/p^r\mathbb{Z})^\times$ und $\ker \simeq \mathbb{Z}/p^{r-1}\mathbb{Z}$
$(1+p)^p = 1 + \binom{p}{1} p + \binom{p}{2} p^2 + ...$
Öööööh, kein peil mehr... *g*

Partialbruchzerlegung von $\frac{1}{1+x^4}$ in $\mathbb{C}$
Zerlegung in Linearfaktoren: Nullstellen von $1 + x^4$ sind jede zweite 8. Einheitswurzel
$\Rightarrow \zeta = e^{\frac{2\pi i}{8}}$ etc. $\Rightarrow x^4 + 1 = (x - \zeta)(x - \zeta^3)(x - \overline{\zeta})(x - \overline{\zeta}^3)$

$$\Rightarrow \frac{1}{1+x^4} = \frac{a}{x-\zeta} + \frac{b}{x-\zeta^3} + \frac{c}{x-\overline{\zeta}} + \frac{d}{x-\overline{\zeta}^3} \text{ mit } a, b, c, d \in \mathbb{C}$$

Polynom ist reell $\Rightarrow c = \overline{a}, d = \overline{b}$
Multiplizieren mit $x - \zeta$:

$$a = \frac{1}{(x-\zeta^3)(x-\overline{\zeta})(x-\overline{\zeta}^3)} - (bla)(x-\zeta) = \frac{1}{(\zeta-\zeta^3)(\zeta-\zeta^7)(\zeta-\zeta^5)}$$

(weil $\overline{\zeta} = \zeta^7$ und ζ für x eingesetzt)

$$(\zeta-\zeta^3)(\zeta-\zeta^7)(\zeta-\zeta^5) = \zeta^3 - \zeta^7 - \zeta + \zeta^5 - \zeta^5 + \zeta + \zeta^3 - \zeta^7 = 2\zeta^3 - 2\zeta^7 = 4\zeta^3$$

(hö?)

Blatt 10 Aufgabe 3: char$K \neq 2, [L:K] = 2 \Rightarrow L/K$ Galois, Gal$(L/K) = \mathbb{Z}/2\mathbb{Z}$, $A := \{\alpha \in L \setminus K \mid \alpha^2 \in K\} = \{\alpha \in L \mid \alpha \neq 0 \wedge \gamma(\alpha) = -\alpha\} =: B$
$\forall \alpha \in L/K : L = K(\alpha) \Rightarrow$Irr$(\alpha, K)$ hat Grad $2 \Rightarrow L/K$ ist ZFK $\Rightarrow L/K$ normal
Char$K \neq 2 \Rightarrow \frac{d}{dx}Irr(\alpha, K) \neq 0 \Rightarrow L/K$ separabel $\Rightarrow$ Galois $\Rightarrow$ Gal$(L/K) = \mathbb{Z}/2\mathbb{Z}$
$\alpha \neq 0$, $\gamma(\alpha) = -\alpha \Rightarrow \gamma(\alpha)^2 = \alpha^2 \Rightarrow \alpha^2 \in K$, aber $\alpha \notin K$ (weil char$\neq 2$) $\Rightarrow B \subset A$
$\alpha^2 \in K \Rightarrow \gamma(\alpha^2) = \alpha^2 \Rightarrow \gamma(\alpha)^2 = \alpha^2 \Rightarrow \gamma(\alpha) = \pm\alpha$
Aber $\alpha \notin K \Rightarrow \gamma(\alpha) \neq \alpha \Rightarrow \gamma(\alpha) = -\alpha \Rightarrow A \subset B$

Zerlegung in Quadratebla: $p \in \mathbb{N}$ prim $\equiv 3(\text{mod}4) \Rightarrow$ prim in $\mathbb{Z}[i]$
$p \equiv 1(\text{mod}4) \Rightarrow \exists x, y : p = x^2+y^2 = (x+iy)(x-iy)$ Beispiel: $5 = 1^2+2^2 = (1+2i)(1-2i)$

Blatt 8 Aufgabe 3: $\mathbb{Z}$: 1. erzeuger 2. linear unabhängig
1. $\frac{F(X)}{G(X)} \in k(X)$. Teile mit rest: $F = G \cdot A + R \Rightarrow \frac{F}{G} = A + \frac{R}{G}$
$\Rightarrow$ oBdA: grad$F <$grad$G$
zerlege $G = P_1^{n_1} \cdot ... \cdot P_r^{n_r}$ in irreduzibel. Wir wollen:

$$\frac{F}{G} - \frac{Q}{P_1^{n_1}} = \frac{HP_1}{G} \text{ mit grad}Q < \text{grad}P_1$$

$$\Leftrightarrow F - Q(P_2^{n_2} \cdot ... \cdot P_r^{n_r}) = HP_1$$

$(P_2^{n_2} \cdot ... \cdot P_r^{n_r})$ und P_1 sind teilerfremd und man findet eine Lösung so dass grad$Q <$gradP_1 (Chinesischer Restsatz)
Behauptung folgt aus Induktion :-)
2. Betrachte $k \subset \overline{k}$ algebraisch abgeschlossen - $\mathbb{Z}$ l.u. in $\overline{k}(X)$
Angenommen:

$$\sum b_n X^k + \sum_{k<\text{grad}P_i,\ \nu>0,\ i} a_i^{k,\nu} X^k P_i^{-\nu} = 0 \Rightarrow \sum_{k<\text{grad}P_i,\ \nu>0} a_i^{k,\nu} X^k P_i^{-\nu} = 0 \text{ für jedes feste } i$$

$\mathbb{Z}$: $X^k P^{-\nu}$ l.u. für feste P

$$\text{grad}P = r : \sum_{\nu=1}^{N} \sum_{k=0}^{r-1} a_{k,\nu} X^k P^{-\nu} = 0 \qquad | \cdot P^N$$

$\Rightarrow \mathbb{Z}$: $P^\nu X^k$ l.u.: offensichtlich.