WS 05/06
Priv.-Doz. Dr. S. Wewers

Algebra I

Inhalt der Vorlesung

I Gruppentheorie

1. Definition von Gruppen und Homomorphismen.
   Beispiele: Permutationsgruppen, die orthogonale Gruppe=Isometrien des $\mathbb{R}^n$, Symmetriegruppe des Tetraeders und des Würfels
2. Nebenklassen, Quotientengruppen.
   Satz: $g^{|G|} = 1$; Bsp.: $S_4/V_4 \cong S_3$
3. Operationen von Gruppen auf Mengen, Bahnengleichung.
   Anwendungen:
   - Auf wieviele Weisen kann man die Seiten eines Tetraeders/Würfels mit n Farben einfärben?
   - Satz von Cauchy: $p|\,|G| \;\Rightarrow\; \exists g : \mathrm{ord}(g) = p$.
4. Auflösbare Gruppen.
   Satz: A_n, S_n sind auflösbar $\Leftrightarrow\; n \leq 4$.
5. Abelsche Gruppen: Zyklische Gruppen, Elementarteilersatz und Hauptsatz über endlich erzeugte abelsche Gruppen.
6. Chinesischer Restsatz, Primitivwurzel mod p^r, die Struktur von $(\mathbb{Z}/n)^\times$.
7. Der diskrete Logarithmus, Diffie-Hellman-Schlüsselaustausch

II Elementare Ringtheorie

1. Ringe, Homomorphismen, Ideale:
   Definition von komm. Ringen, Polynomringe, maximale und Primideale
2. Hauptidealringe:
   euklidische Ringe und der euklidische Algorithmus; Bsp: $\mathbb{Z}, k[X], \mathbb{Z}[i]$.
   Anwendung: $p = a^2 + b^2 \;\Leftrightarrow\; p \equiv 1 \pmod 4$.
3. Teilbarkeit in Integritätsringen:
   irreduzible und Primelemente, faktorielle Ringe, eindeutige Primfaktorzerlegung, ggT, kgV.
   Satz: HIR sind faktoriell; Korollar: Fundamentalsatz der Arithmetik
   Lemma von Gauß, Polynomringe über faktoriellen Ringen,
   Satz: $k[X_1, \ldots, X_n]$ ist faktoriell

4. Irreduzibilität von Polynomen:
   - Fundamentalsatz der Algebra
   - geometrische Interpretation der Irreduzibilität in $\mathbb{C}[X, Y]$
   - Irreduzibilität in $\mathbb{Q}[X]$: Eisensteinkriterium, Reduktion mod p; Bsp: zyklotomische Polynome ϕ_p

III Körper- und Galoistheorie

1. Algebraische Erweiterungen:
   algebraische/transzendente Elemente, Minimalpolynom, Multiplikativität des Körpererweiterungsgrad.
2. Konstruktion mit Zirkel und Lineal:
   Charakterisierung durch Körpererweiterungsgrad, Satz: Das regelmässige n-Eck ist konstruierbar $\Leftrightarrow$ $\varphi(n) = 2^m$.
3. Endliche Körper:
   Existenz und Eindeutigkeit, irreduzible Polynome in $\mathbb{F}_p[X]$
4. Galois-Erweiterungen:
   - Separable Erweiterungen; Kriterium durch formales Ableiten
   - Normale Erweiterungen; Zerfällungskörper, Fortsetzen von Einbettungen
   - Satz: Galois $\Leftrightarrow$ separabel und normal
   - Hauptsatz der Galoistheorie; Bsp: quadratische und kubische Erweiterungen
5. Der Hauptsatz der Galoistheorie:
   - Satz: $K = L^G \Rightarrow L/K$ ist Galois
   - Satz vom primitiven Element
   - Beweis des Hauptsatzes
   - Bsp.: endliche Körper, Kreisteilungskörper
6. Auflösen von Gleichungen durch Radikale:
   - Satz: $f = 0$ auflösbar $\Leftrightarrow$ $G(f)$ auflösbar.
   - Korollar: $f = 0$ auflösbar falls $\deg(f) \leq 4$.
   - Bsp.: $f = x^5 - 16x + 2 = 0$ ist *nicht* auflösbar, da $G(f) = S_5$.