

Concrete Abstract Algebra of Niels Lauritzen

Number theory

- Corollary 1.5.11(i)**
 $(gcd(a,b) = 1, a|c, b|c) \implies ab|c.$ 13
- Corollary 1.5.11(ii)**
 $gcd(a,b) = gcd(a,c) = 1 \implies gcd(a,bc) = 1.$ 13
- Theorem 1.6.4** Chinese Remainder Theorem. 16
- Lemma 1.8.3** (p prime number, $p|ab$) $\implies (p|a \vee p|b).$ 22
- Section 1.8.3** Tells how to compute $\varphi(n).$ 24

Group theory

- Theorem 2.2.8** Lagrange. 53
- Section 2.1.6** For $g \in G, \varphi : G \rightarrow G$ with $\varphi(x) = gx$ is bijective. 56
- Lemma 2.3.6**
 $(H, K \subseteq G, H \text{ normal}) \implies HK \subseteq G.$ 66
- Proposition 2.4.9** $f : G \rightarrow K$ group homomorphism 70
- Proposition 2.4.9(i)** $f(G) \subseteq K.$ 70
- Proposition 2.4.9(ii)** $Ker(f) \subseteq G$ normal. 70
- Proposition 2.4.9(iii)** f injective $\Leftrightarrow Ker(f) = \{e\}.$ 70
- Proposition 2.6.3** talks about group element order. 73
- Proposition 2.7.2** (G group, $|G| = p$ prime number)
 $\implies G \cong Z/pZ$ cyclic. 74
- Proposition 2.7.4**
 talks about cyclic groups and subgroups. 75
- Lemma 2.8.1** ($M, N \subseteq G$ normal, and $M \cap N = \{e\}$)
 $\implies M \times N \cong MN.$ 77
- Proposition 2.8.2** The group version of the Chinese. 77

Permutations

- Section 2.9** $|S_n| = n!.$ 78
- Section 2.9.3** $|A_n| = \frac{n!}{2}.$ 85
- Section 2.9.1** $ord(k\text{-cycle}) = k$
 (look just above example 2.9.3, p. 80). 79
- Proposition 2.9.5** $\sigma = \sigma_1 \dots \sigma_r, \sigma_i$ disjoint,
 $ord(\sigma) = lcm\{\sigma_1, \dots, \sigma_r\}.$ 80
- Proposition 2.9.14**
 σ is a product of $\geq n(\sigma)$ simple transpositions. 84
- Proposition 2.9.16** sgn is a group homomorphism. 85
- Proposition 2.9.17** $sgn(k\text{-cycle}) = (-1)^{k-1}.$ 86
- Section 2.10.2**
 $\forall \sigma_1, \sigma_2 \in S_n : \exists \tau \in S_n : \tau \sigma_1 \tau^{-1} = \sigma_2.$ 98

Sylow-subgroups, pp. 101-104

Ring theory

- Proposition 3.2.2** $d \in Z.$ Then $(Z/dZ)^*$ is abelian with order $\phi(d).$ 117
- Proposition 3.2.7** An ideal $I \subseteq R$ is maximal $\Leftrightarrow R/I$ is a field. 119
- Proposition 3.3.2** ($f : R \rightarrow S$ ring homomorphism) $\implies (g : R/Ker(f) \rightarrow f(R)$ ring isomorphism). 120
- Proposition 3.3.7** R finite domain $\implies (R$ field, $char R = p$ prime number). 121
- Theorem 3.5.7** A principal ideal domain is a unique factorization domain. 129

Polynomium rings

- Proposition 4.2.2**
 Conditions for $deg(fg) = deg(f) + deg(g).$ 148
- Proposition 4.2.4**
 $f, d \in R[X] \exists q, r \in R[X] : f = qd + r.$ 148
- Theorem 4.3.5** $f = 0$ then $f = q(X - \alpha_1)^{v_{\alpha_1}(f)} \dots (X - \alpha_r)^{v_{\alpha_r}(f)}, V(q) = \emptyset.$ 152
- Lemma 4.3.8**
 $f, g \in R[X]$ i) $f^2 | g \implies f | D(g).$ ii) $v_{\alpha}(f) > 1 \Leftrightarrow \alpha$ root of f and $D(f).$ 154
- Theorem 4.5.3** F field, $G \subseteq F^*$ finite subgroup. Then G is cyclic. 158
- Proposition 4.6.3(i)**
 $(f$ maximal ideal) $\Leftrightarrow (f$ irreducible).
 $(f$ irreducible) $\implies (F[X]/f$ field). 162
- Proposition 4.6.3(ii-v)**
 Defines when f is a unit or irreducible. 162
- Proposition 4.6.7** ($g \in R[X]/f, f$ monic of $deg \geq n > 0$) $\implies (g = b_0 X^0 \dots b_{n-1} X^{n-1}$ uniquely). 165

Gröbner bases

- Proposition 5.3.1** Division algorithm. 194
- Theorem 5.6.8** $F(f_1, \dots, f_m)$ GB $\Leftrightarrow (S(f_i, f_j) \rightarrow_F 0$ for $1 \leq i < j \leq m).$ 208
- Corollary 5.6.9**
 $(F = (f_1, \dots, f_m)$ GB) \Leftrightarrow for all $1 \leq i < j \leq m$ we have $S(f_i, f_j)^F = 0.$ 208
- Lemma 5.7.3** ($f, g \in R, gcd(in_{\leq}(f), in_{\leq}(g)) = 1$) $\implies S(f, g) \rightarrow_{(f,g)} 0.$ 210
- Theorem 5.9.1** Tells about $G \cap k[X_1, \dots, X_i]$ being a GB for $I \cap k[X_1, \dots, X_i].$ 215

Good definitions

- Definition 2.2.1** Subgroup. 61
- Definition 2.4.1** Group homomorphism. 68
- Definition 2.5.1** Group isomorphism. 71
- Definition 3.3.1** Ring, subring, etc. 112
- Section 3.3** Ring homo- and isomorphism. 119