Modern Computer Algebra

Exercises to Chapter 25: Fundamental concepts

11 May 1999

JOACHIM VON ZUR GATHEN
and
JÜRGEN GERHARD

Universität Paderborn

CAMBRIDGE
UNIVERSITY PRESS

25.1 Show that any subgroup of a group G contains the neutral element 1 of G.

25.2 Show that cyclic groups are commutative.

25.3 Let $G = \mathrm{GL}_2(\mathbb{R})$ be the group of invertible 2×2 matrices over $\mathbb{R}$. Show that

$$U = \left\{ A \in G : A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

is a subgroup of G.

25.4 Let $E_{12} = \{e^{\pi i j/6} : 0 \le j < 12\} \subseteq \mathbb{C}$, where $i = \sqrt{-1}$ is the imaginary unit.

(i) Show that $a^{12} = 1$ holds for all $a \in E_{12}$. (That is why the elements of E_{12} are called the 12th roots of unity.)

(ii) Mark the elements of E_{12} on the unit circle in the complex plane.

(iii) Show that E_{12} is a commutative group with respect to the multiplication of complex numbers.

(iv) Show that the set $E_4 = \{e^{\pi i k/2} : 0 \le k < 4\}$ of 4th roots of unity is a subgroup of E_{12}. Highlight the elements of E_4 in your drawing.

(v) Determine all (left) cosets with respect to E_4.

(vi) Set up the multiplication table of the factor group E_{12}/E_4.

25.5 Show that the set $E = \{z \in \mathbb{C}^\times : \exists n \in \mathbb{N}_{\ge 1}\ z^n = 1\} \subseteq \mathbb{C}^\times$ of all complex roots of unity is a subgroup of $(\mathbb{C}^\times, \cdot)$.

25.6 S_4 is the set of all bijective maps (permutations) from $\{1, \ldots, 4\}$ to itself. We represent an element $\pi \in S_4$ as $(\pi(1)\,\pi(2)\,\pi(3)\,\pi(4))$, and examine the following subset:

$$V = \{(1234),\ (4321),\ (2143),\ (3412)\}.$$

(i) Draw cycle diagrams for the elements of V.

(ii) Show that V together with the composition $\circ$ of maps is a subgroup of S_4, and compute the multiplication table of V.

25.7 Let $G = \{x \in \mathbb{Q} : 0 \le x < 1\}$.

(i) Show that G together with the operation

$$x \oplus y = \begin{cases} x + y & \text{falls } 0 \le x + y < 1 \\ x + y - 1 & \text{falls } x + y > 1 \end{cases}$$

is a commutative group with infinitely many elements.

(ii) Show that all elements of G have finite order. (Hint: express $x \in G$ as a fraction.)

(iii) Prove that G is isomorphic to the factor group $\mathbb{Q}/\mathbb{Z}$ with respect to addition.

25.8 (i) Show that the set $S_{\mathbb{R}} = \{ f : \mathbb{R} \longrightarrow \mathbb{R},\ f \text{ bijective}\}$ is a group with respect to the composition $\circ$ of maps. Is this group commutative?

(ii) For $a, b \in \mathbb{R}$ let $f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}$ be the function given by $f_{a,b}(x) = ax + b$. Show that the set $G = \{ f_{a,b} : a, b \in \mathbb{R},\ a \neq 0\}$ is a subgroup of $S_{\mathbb{R}}$. Is G commutative?

(iii) Show that $H = \{ f_{1,b} : b \in \mathbb{R}\}$ is a commutative subgroup of G.

25.9 (i) Are S_3 and $(\mathbb{Z}_6, +)$ isomorphic? Explain your answer.

(ii) Show that $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $\varphi(x) = 3x$ is a homomorphism with respect to addition in $\mathbb{Z}$.

(iii) Let $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$. Show that $\varphi : \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$ with $\varphi(x) = 3x$ is not a homomorphism with respect to multiplication in $\mathbb{R}$.

25.10 Which of the following maps are group homomorphisms? Determine the kernel and the image of all homomorphisms.

(i) $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^\times, \cdot)$, $\varphi(x) = e^{ix}$.

(ii) $\varphi : (\mathbb{C}^\times, \cdot) \longrightarrow (\mathbb{R}^\times, \cdot)$, $\varphi(x) = |x|$.

(iii) $\varphi : (\mathbb{Z}_{17}^\times, \cdot) \longrightarrow (\mathbb{Z}_{17}^\times, \cdot)$, $\varphi(x) = x^2$.

(iv) $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, $\varphi(x) = x + 17$.

(v) $h : (\mathbb{Z}_3, +) \longrightarrow (\mathbb{Z}_4, +)$, $h(0) = 0$, $h(1) = 1$, $h(2) = 2$.

25.11 Let U be a subgroup of the group G. Show that $U \cdot U = U$, where $U \cdot U = \{u_1 u_2 : u_1, u_2 \in U\}$.

25.12 Let $p \in \mathbb{N}$ be prime and $U < \mathbb{Z}_p$ a subgroup of the additive group $(\mathbb{Z}_p, +)$ with $U \neq \{0\}$. Show that $U = \mathbb{Z}_p$.

25.13 Prove:

(i) If the order of a group G is prime, then there exists a primitive element g in G, such that $\langle g \rangle = G$.

(ii) If H and K are subgroups of the finite group G and $\gcd(\#H, \#K) = 1$, then $H \cap K = \{e\}$. (Hint: Show first that $H \cap K$ is a subgroup of G.)

25.14 Show that any cyclic group G of order n is isomorphic to $\mathbb{Z}_n$ (with addition modulo n). Thus there is essentially only one cyclic group of order n.

25.15 Let $\varphi : G \longrightarrow H$ be a homomorphism of multiplicative groups. Show that $\ker \varphi$ is a normal subgroup of G (this means that it is a subgroup and $g^{-1}ag \in \ker \varphi$ for all $g \in G$ and $a \in \ker \varphi$) and $\varphi(G)$ is a subgroup of H. What is the analogous statement for rings?

25.16 Let G be a group. Prove:

(i) G is commutative if and only if the inversion mapping $x \longmapsto x^{-1}$ is a group homomorphism.

(ii) G is commutative if and only if the squaring mapping $x \longmapsto x^2$ is a group homomorphism.

(iii) If $x^2 = 1$ for all $x \in G$, then G is commutative.

25.17 Let G and H be two groups and $\varphi: G \longrightarrow H$ a group homomorphism. Show:

(i) If $g \in G$ and $n \in \mathbb{N}$, then $\varphi(g^n) = \varphi(g)^n$.

(ii) If $g \in G$, then $\mathrm{ord}(\varphi(g)) \mid \mathrm{ord}(g)$. Does equality hold in general?

(iii) If φ is surjective and G is commutative, then H is commutative.

25.18 Let G and H be two groups.

(i) Let $\varphi: G \longrightarrow H$ be a map with $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. Show that $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$ holds for all $g \in G$.

(ii) Show that a homomorphism $\varphi: G \longrightarrow H$ is injective if and only if its kernel is $\ker \varphi = \{e_G\}$.

25.19 (i) Determine all homomorphisms $S_3 \longrightarrow \mathbb{Z}_5$.

(ii) Show: For $n, m \in \mathbb{N}_{>0}$, $(\mathbb{Z}_n, +)$ has a subgroup isomorphic to $(\mathbb{Z}_m, +)$ if and only if m divides n.

(iii) Let $p \in \mathbb{N}$ be prime and G, H finite groups with $\#G = p$. If $\varphi: G \longrightarrow H$ is a homomorphism, then either $\varphi(g) = e_H$ for all $g \in G$ or φ is injective.

25.20* Show that for $k, n \in \mathbb{N}$, the map $\varphi: \mathbb{Z}_n \longmapsto \mathbb{Z}_n$ with $\varphi(a) = ka$ is a group automorphism of $(\mathbb{Z}_n, +)$ if and only if $\gcd(k, n) = 1$.

25.21* We examine the set G of the following eight 2×2 matrices:

$$D_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, D_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, D_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, D_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, S_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, S_3 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

(i) The matrices $D_0, \ldots, D_3$ induce rotations of the real plane $\mathbb{R}^2$ around the origin, and $S_0, \ldots, S_3$ induce reflections whose axes contain the origin. Determine the rotation angles and the reflection axes.

(ii) G is a group with respect to matrix multiplication. Let U be the subset of all matrices in G that map the x-axis to itself (not necessarily pointwise). Show that U is a subgroup of G and determine the multiplication table of U.

(iii) Determine all left cosets with respect to U.

(iv) We consider the square with endpoints $p_1 = \binom{1}{1}$, $p_2 = \binom{-1}{1}$, $p_3 = \binom{-1}{-1}$, and $p_4 = \binom{1}{-1}$. Each matrix $A \in G$ induces a permutation $\pi \in S_4$ of the four points via $p_{\pi(i)} = A \cdot p_i$. For each $A \in G$, find the corresponding permutation. Which subset of S_4 corresponds to U?

(v) Compute the order of every element of G. Does G have a primitive element?

(vi) Show that G is generated by the set $\{D_1, S_0\}$, so that every element of G can be represented as a sequence of rotations by 90° and reflections about the x-axis.

25.22 Determine all ideals of the ring $\mathbb{Q}$.

25.23 Show that $I = \{4x + 6y : x, y \in \mathbb{Z}\}$ in an ideal in the ring $\mathbb{Z}$.

25.24 Let $I = \{f \in \mathbb{R}[x] : f(5) = 0\}$ be the set of real polynomials having 5 as a root.

(i) Show that I is an ideal in $\mathbb{R}[x]$.

(ii) Find an isomorphism $\mathbb{R}[x]/I \longrightarrow \mathbb{R}$.

25.25 The set $R = \mathbb{R} \times \mathbb{R}$ together with componentwise addition and multiplication is a ring.

(i) Find an isomorphism of the additive groups of R and $\mathbb{C}$, including a proof.

(ii) Show that there is no ring isomorphism from R onto $\mathbb{C}$. (Hint: R is not an integral domain.)

25.26 Take $R = \{2k : k \in \mathbb{Z}\}$ together with the usual addition and multiplication. Show:

(i) $(R, +)$ is a group, and "$\cdot$" is associative, commutative, and distributive.

(ii) There is no neutral element with respect to multiplication in R.

25.27 Which of the following sets I are ideals in the ring R?

(i) $I = \mathbb{Z}$ and $R = \mathbb{Q}$.

(ii) $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ and $R = \mathbb{R}^{2\times 2}$.

(iii) $I = \{0, 3\}$ and $R = \mathbb{Z}_6$.

(iv) $I = \{(a, 0) : a \in \mathbb{R}\}$ and $R = \mathbb{R} \times \mathbb{R}$ together with componentwise addition and multiplication.

25.28 Which of the following claims are true, which are false (give a short explanation)?

(i) $\mathbb{Z}_{13}^{\times}$ has a subgroup with 5 elements.

(ii) If p is prime, then the ring $\mathbb{Z}_p$ has exactly two ideals.

(iii) There is exactly one group homomorphism $\varphi : (\mathbb{Z}_3, +) \longrightarrow (\mathbb{Z}_5, +)$.

25.29 Let R be a ring. Show that the set $R^{\times} = \{r \in R : \exists s \in R \; rs = 1\}$ of all invertible ring elements is a multiplicative group.

25.30 Let R be a ring (commutative, with 1) and $a, b \in R$. Show that $a \mid b$ if and only if $b \in \langle a \rangle$.

25.31 Let R be a ring and consider R^R, the set of all functions $R \longrightarrow R$. We endow R^R with a ring structure in a natural way: if $f, g \in R^R$, then

$$\begin{aligned}
(f+g)(x) &= f(x) + g(x), \\
(fg)(x) &= f(x)g(x), \\
(-f)(x) &= -f(x), \\
1(x) &= 1, \\
0(x) &= 0,
\end{aligned}$$

where the right-hand side operations are those of R. (The verification that R^R under the above operations is a ring is trivial.) Which of the following properties of R are carried over to R^R?

(i) R has characteristic $m \in \mathbb{N}$,

(ii) R is commutative,

(iii) R is an integral domain.

25.32 Prove that if $z \in \mathbb{Z}[i]$ is a Gaussian integer and its norm $N(z)$ is a prime in $\mathbb{Z}$, then z is irreducible in $\mathbb{Z}[i]$. Verify that $1+i, 1+2i$, and $2-3i$ are all irreducible in $\mathbb{Z}[i]$.

25.33 Show that 6 and $2+2\sqrt{-5}$ have no gcd in $\mathcal{O}_{-5}$.

25.34* Let R be an integral domain and $p \in R$. Prove:

(i) If p is prime, then p is irreducible.

(ii) If any two nonzero elements of R have a gcd and p is irreducible, then p is prime.

25.35* Show that if I is an ideal in $R = \mathbb{R}^{2\times 2}$ and $I \neq \{0\}$, then $I = R$. To prove this, show that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I$.

25.36 Prove or disprove:

(i) If U and V are subgroups of a group G, then so is $U \cup V$.

(ii) If U and V are subgroups of a group G, then so is $U \cap V$.

(iii) If F is a field, then so is $F[x]$.

(iv) If R is a ring, then so is $R[x]$.

(v) If R is an integral domain, then so is $R[x]$.

(vi) $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field.

25.37* Let R be a commutative ring. Show that the following claims are true if R is an integral domain, and give counterexamples where R has zero divisors.

(i) The degree formula $\deg(fg) = \deg f + \deg g$ holds for nonzero polynomials $f, g \in R[x]$.

(ii) The units of $R[x]$ are exactly the units of R.

(iii) A polynomial $f \in R[x] \setminus \{0\}$ has at most $\deg f$ roots. Hint: Show first that $x-a$ divides f if $a \in R$ is a root of f (this is true in arbitrary commutative rings).

25.38* Show that any finite extension field E of a field F is algebraic.

25.39** Let $(G,\cdot) < (H,\cdot)$ be commutative groups. An element $x \in H$ is **algebraic** over G if it satisfies an equation of the form $x^n = g$ for some $n \in \mathbb{N}$ and $g \in G$, otherwise it is **transcendental**. H is algebraic over G if every element of H is. H is **algebraically closed** if every equation is solvable in H, so that for all $h \in H$ and $n \in \mathbb{N}$ there exists an $x \in H$ such that $x^n = h$. H is an **algebraic closure** of G if H is algebraic over G and algebraically closed. (Do not confuse these notions with the corresponding ones for field extensions.)

(i) Show that $(\mathbb{Q},+)$ is an algebraic closure of $(\mathbb{Z},+)$.

(ii) Let $E=\{z\in\mathbb{C}: \exists n\in\mathbb{N}\ z^n=1\}\subseteq\mathbb{C}^\times$ be the group of all complex **roots of unity** as in Exercise 25.5. Show that $(E,\cdot)$ is algebraically closed and that $E\cong\mathbb{Q}/\mathbb{Z}$.

(iii) Describe the subgroup of $\mathbb{Q}/\mathbb{Z}$ that is isomorphic to the subgroup $T=\{z\in E: \exists k\in\mathbb{N}\ z^{2^k}=1\}$ of E. Is T algebraically closed?

(iv) Show that $(\mathbb{Q}_{>0},\cdot)$ is not algebraically closed. Describe an algebraic closure G of $(\mathbb{Q}_{>0},\cdot)$ in $(\mathbb{R}_{>0},\cdot)$. Are $(\mathbb{Q},+)$ and $(G,\cdot)$ isomorphic? (Hint: for all $a,b\in\mathbb{Q}$ there exist $m,n\in\mathbb{Z}$ such that $ma+nb=0$.)

(v) Let $H_2=\langle 2\rangle$ be the subgroup generated by 2 in $\mathbb{Q}_{>0}$ and K_2 its algebraic closure in G. Show that $(K_2,\cdot)$ and $(\mathbb{Q},+)$ are isomorphic. Show that 3 is transcendental over K_2.

(vi) Show that G is the **direct sum** of the corresponding subgroups K_p for all primes $p\in\mathbb{N}$, so that every $g\in G$ can be uniquely written as a finite product of elements of the K_p.

25.40 Consider the field $K=\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$.

(i) What is its characteristic?

(ii) What is its order?

(iii) Explicitly list the elements of the field and, for two of them, give their multiplicative inverses.

(iv) Give an example of an irreducible polynomial over this field of degree 2. Explain why your polynomial is irreducible.

25.41 For $p=7,11$, and 13, find the smallest positive integer generating the multiplicative group $\mathbb{F}_p^\times$, and determine how many of the integers $1,2,3,\ldots,p-1$ are generators.

25.42 Let $p\in\mathbb{N}$ be prime, $q=p^k$ for some $k\in\mathbb{N}_{>0}$, and $\mathbb{F}_q$ a finite field with q elements. Show:

(i) If x,y are indeterminates over $\mathbb{F}_q$ and $l\in\mathbb{N}$, then $(x+y)^{p^l}=x^{p^l}+y^{p^l}$.

(ii) If $f\in\mathbb{F}_q[x]$, then $f^q=f(x^q)$.

(iii) If $f\in\mathbb{F}_q[x]$, then $f^q-f=\prod_{u\in\mathbb{F}_q}(f-u)$.

25.43* Let $p\in\mathbb{N}$ be prime, $r\in\mathbb{N}_{>0}$, and $q=p^r$. Under what conditions on p and r is *every* element of $\mathbb{F}_q$ except 0 and 1 a generator of the multiplicative group $\mathbb{F}_q^\times$? Under what conditions is every element $\neq 0,1$ either a generator or the square of a generator?

25.44 Prove that there is no inner product $\star\colon\mathbb{F}_2^2\times\mathbb{F}_2^2\longrightarrow\mathbb{F}_2$.

25.45 Prove (5).

25.46 Let $q\in\mathbb{R}_{>0}$ or $q=\infty$, and $S_q=\{v\in\mathbb{R}^2: \|v\|_q=1\}$. Then S_2 is the unit circle. What is S_1 and S_∞? Describe how S_q changes when q varies in the interval $(0,\infty]$.

25.47* Prove that $\|a\|_\infty = \lim_{q \longrightarrow \infty} \|a\|_q$ for all $a \in \mathbb{C}^n$.

25.48 Let X and Y be two discrete random variables. Prove that $\mathrm{var}(X+Y) = \mathrm{var}(X) + \mathrm{var}(Y)$ if and only if X and Y are independent.

25.49 Let $k \in \mathbb{N}$ and $c(n) = n(\log n)^k$ for $n \in \mathbb{N}$. Prove

$$\sum_{0 \leq i \leq \lceil \log n \rceil} c(2^i) \in O(c(n)).$$

25.50 Let $f, g\colon \mathbb{N} \longrightarrow \mathbb{R}$ be eventually positive. Prove the equality $O((f+g)^2) = O(f^2 + g^2)$.

25.51 Let $f\colon \mathbb{N} \longrightarrow \mathbb{R}$ be eventually positive with $\lim_{n \longrightarrow \infty} f(n) = 0$. Prove that $1/(1+O(f)) = 1 + O(f)$.