Exercises for TATA55, Abstract Algebra

September 1, 2022

1 Sets, Relations, Binary operations

Let X be a set, $\mathcal{P}(X)$ the set of all subsets of X. Let $\mathcal{REL}$ be the set of relations on X, i.e., subsets of $X \times X$. If A, B are relations on X, their composition is defined by

$$B \circ A = \{\, (x,z) \in X \times X \,|\, \exists y \in X : \, (x,y) \in A \text{ and } (y,z) \in B \,\}.$$

The domain of A is $\{\, x \in X \,|\, \exists y \in X : (x,y) \in A \,\}$, and the range is $\{\, y \in X \,|\, \exists x \in X : (x,y) \in A \,\}$.

1. Judson, section 1.3, exercise 17,19,22,25-26
2. Svensson, section 1.1, exercise 5-6,9,12
3. Svensson, section 1.3, exercise 6,8
4. Svensson, section 1.4, exercise 1,5-7
5. Show that $\cup$, $\cap$, Δ are associative binary operations on $\mathcal{P}(X)$.
6. Is $(A, B) \mapsto A \cup (A \cap B)$ associative?
7. Is $\setminus$ associative?
8. Is composition of relations associative?
9. Call a relation f a partial function if

   $$(x, y_1) \in f,\, (x, y_2) \in f \qquad \Longrightarrow \qquad y_1 = y_2.$$

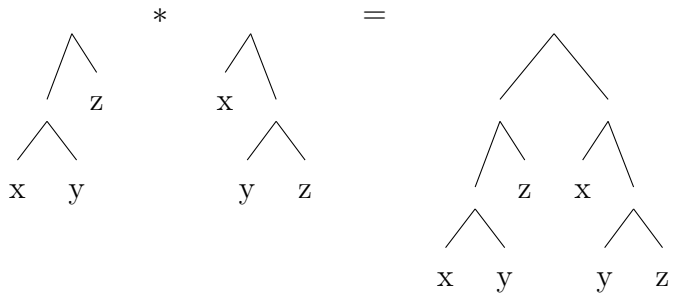
   Show that composition of partial functions yield a partial function. Is composition of partial functions associative?
10. A partial function is total (or just a function) if its domain is the whole of X. Show that the composition of two functions is a function. Is composition associative?

11. Let T be the set of rooted complete binary trees, with leaves labeled with elements in X. This is the smallest set such that

    (a) If $x \in X$ then $x \in T$,

    (b) If $A, B \in T$ then  is in T.

    Now define the following binary operation on T by defining $A * B$ as the tree above. As an example, if $x, y, z \in X$, then



    Show that this binary operation is not associative.

12. Let S be the smallest set of strings on the alphabet $X \cup \{*, (,)\}$ such that

    (a) $x \in X \implies x \in S$,

    (b) $u, v \in S \implies (u * v) \in S$.

    Introduce a binary operation on S by defining the product of the well-formed strings $u, v \in S$ to be the string $(u * v) \in S$. Show that there is a bijection between T and S which preserves the binary operations.

13. We denote the set of all finite strings $x_{i_1} \cdots x_{i_n}$, with $x_i \in X$, by X^*. Here we include the empty string ϵ, which has length zero. The concatenation of $x_{i_1} \cdots x_{i_n}$ and $y_{j_1} \cdots y_{j_m}$ is the string $x_{i_1} \cdots x_{i_n} y_{j_1} \cdots y_{j_m}$. For instance, if $X = a, b$,$u = aa$, $v = baa$, then $uv = aabaa$.

    (a) Show that X^* is a monoid. Show that it is only commutative if $|X| = 1$.

    (b) Let $X = a, b$ and let $X_n \subset X^*$ be the subset of words of length n. Determine $|X_n|$.

    (c) Let $A \subset X^*$ be the subset of words that ca be written as $u * aa * v$, with $u, v \in X^*$. Determine $|A \cap X_n|$.

    (d) Let $B \subset X^*$ be the subset of words that can be written as $u * ab * v$, with $u, v \in X^*$. Determine $|B \cap X_n|$.

14. Let n be a positive integer, and let M_n denote the set of all $n \times n$ complex matrices, with matrix multiplication. Show that M is a monoid.

15. Show that the following binary operation on M is neither commutative nor associative: $[A, B] = AB - BA$. Show however that $[B, A] = -[A, B]$, and

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0.$$

16. If $n = 2$, show that $[[A, B]^2, C] = 0$.

17. Let $|X| = n < \infty$, and let $f : X \to X$. Let V be the free $\mathbb{C}$-vector space on X, with a basis consisting of a $\mathbf{e}_x$ for each $x \in X$. Define a linear map

$$T_f : V \to V$$
$$\sum_{x \in X} c_x \mathbf{e}_x = \sum_{x \in X} c_x \mathbf{e}_{f(x)}$$

Show that $T_g \circ T_f = T_{g \circ f}$.

18. Let M_f be the matrix of T_f w.r.t the basis $\{\mathbf{e}_x\} x \in X$. Show that M_f is a zero-one matrix with exactly one one in each column, and that every such matrix is the matrix of some T_f. Show that $M_g M_f = M_{f \circ g}$, and conclude that the product of two zero-one matrices with precisely one one i each column is again such a matrix. Show that the determinant of M_f is 0,1, or -1.

19. It is shown in the textbook that an equivalence relation $\sim$ on X determines, and is determined by, a partition of X into disjoint subsets, the equivalence classes. Denote by $Y = X/\sim$ the set of all equivalence classes. There is a natural projection

$$\pi : X \to Y$$
$$pi(x) = [x]_\sim$$

mapping each element to its equivalence class.

The axiom of choice allows us to construct a transversal, i.e., a subset $T \subset X$ containing precisely one element from each equivalence class in X. Show that such a transversal gives a map

$$\sigma : Y \to X$$

satisfying $\pi \circ \sigma = 1_Y$, $\sigma \circ \pi \circ \sigma \circ \pi = \sigma \circ \pi$, i.e., $\sigma \circ \pi$ is a normal form on X.

Conversely, show that any map σ as above determines a transversal.

20. Let A be a finite set with n elements, and let $f : A \to A$ be a map. Define a digraph G with vertex set A, and with a directed edge $a \to b$ iff $f(a) = b$.

(a) For $n = 5$, draw the graph associated to

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 1 \end{bmatrix} \quad \text{and} \quad g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 3 \end{bmatrix}$$

(b) Show that every vertex in G has outdegree 1. Show that f is invertible iff every vertex in G has indegree 1.

(c) Pick $a \in A$. Show that the sequence $f^{(k)}(a)$, $k = 0, 1, 2, \ldots$ is eventually periodic. Is $f^{(k)}$, $k = 0, 1, 2, \ldots$ eventually periodic?

21. Let M be a monoid, and let $x \in M$. Suppose that there exists positive integers $0 < n < m$ such that $x^n = x^m$. Show that there are positive integers N, s such that, for all non-negative integers a, b, it holds that

$$x^{N+a} = x^{N+b} \quad \Longleftrightarrow \quad a \equiv b \mod s$$

2 The integers, induction, divisibility, gcd, Bezout

1. Judson, section 2.3, exercise 8,13-14,18,27
2. Svensson, section 1.2, exercise 6-7,9,11,14
3. if $a \,|x$ and $b \,|x$ and $\gcd(a, b) = 1$, show that $ab \,|x$.
4. The extended Euclidean algorithm works as follows: let $0 < b \leq a$ be integers. Put $x_0 = 1$, $y_0 = 0$,$x_1 = 0$,$y_1 = 1$.

   Suppose that x_i, y_i have been determined for $0 \leq i \leq n$. Put $z_i = ax_i + by_i$, and use the division algorithm to write

   $$z_n = kz_{n-1} + r, \qquad 0 \leq r < z_{n-1}.$$

   Put

   $$x_{n+1} = x_n - kx_{n-1}$$
   $$y_{n+1} = y_n - ky_{n-1}$$

   Show that z_i decreases, and that for some N we have that

   $$ax_N + by_N = \gcd(a, b).$$

5. Solve the Diophantine equation

   $$15x + 25y = 100$$

6. Solve the Diophantine equation

$$15x + 25y + 20z = 100$$

7. Solve the equation

$$5x \equiv 8 \mod 3$$

8. Solve the equation

$$10x \equiv 4 \mod 6$$

9. Solve the equation

$$10x + 4y \equiv 4 \mod 6$$

10. Sove the system of congruenses

$$\begin{aligned} x &\equiv 3 \mod 11 \\ x &\equiv -3 \mod 13 \end{aligned}$$

3 Groups, elementary properties and examples

1. Judson, section 3.4, exercise 2,6-7,10,14,26-27,39-41,46,53-54
2. Svensson, section 3.1, exercise 2,3,5,7
3. Svensson, section 3.2, exercise 5,6
4. Svensson, section 3.4, exercise 4-6,9
5. Svensson, section 3.5, exercise 2,10-13
6. Let G be a group. Show that $\emptyset \neq H \subseteq G$ is a subgroup iff $xy^{-1} \in H$ for all $x, y \in H$.
7. Let p be an odd prime number. Show that the set of matrices

$$G = \left\{ \left. \begin{bmatrix} 1 & a & -a & b \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \right| a, b \in \mathbb{Z}_p \right\}$$

   is (under multiplication) a finite abelian group.

8. If G is a group and $g_1, g_2 \in G$, then these elements are said to be conjugate if there exists an element $h \in G$ such that $g_1 = hg_2h^{-1}$.

   (a) Show that this is an equivalence relation on G.

(b) Is the element h necessarily unique?

(c) Do conjugate elements always have the same order?

9. Let $n \geq 3$ be an integer, and put $H_n = \{ (\cos(2k\pi/n), \sin(2k\pi/n)) | k \in \mathbb{Z} \}$. Let K_n be the convex hull of H_n (that is, K_n is the regular n-gon that has H_n as its set of vertices). Let D_n be the set of those linear isometries of the plane that fulfill that $F(H_n) = H_n$. Recall the complete classification of linear isometries of the plane: these are the rotations (orientation preserving, have determinant 1), and the reflections in lines through the origin (orentation-reversing, have determinant -1).

   (a) Show that the linear isometries of the plane form a group under composition, and that D_n is a subgroup.

   (b) Show that D_n is also the set of linear isometries that preserve K_n.

   (c) Show that, for each vertex $h \in H_n$, there is exactly one rotation in D_n that maps $(1, 0)$ to h. Similarly, show that there is exactly one reflection in D_n that maps $(1, 0)$ to h. Conclude that $|D_n| = 2n$.

   (d) Show that any two rotations commute, and that any two reflections are conjugate.

10. In $\mathbb{R}^3$, the linear isometries are the rotations (around a line through the origin) and the reflections (in a plane through the origin). Let K be the cube with vertices in

$$\{ (x, y, z) | x, y, z \in \{-1, 1\} \}.$$

    Let R be the set of **rotations** that preserve K.

   (a) Show that R is a group with 24 elements.

   (b) Show that there are precisely 8 elements of order 3, corresponding to rotations by $2\pi/3$ radians around an axis through two diametrically opposed vertices, and all these rotations are conjugate, but need not commute.

   (c) What are the elements of order 4? Are they all conjugate?

   (d) What about the elements of order 2?

   (e) What other order do the elements in R have?

11. Let G be a group, and let A, B be subgroups of G. Put

$$AB = \{ ab | a \in A,\, b \in B \}, \quad BA = \{ ba | a \in A,\, b \in B \}.$$

    Show that AB is a subgroup if and only if $AB = BA$.

12. Let G be a group, and suppose that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Show that G is abelian.

13. What if, for some positive integer j, $(ab)^j = a^j b^j$ and $(ab)^{j+1} = a^{j+1}b^{j+1}$ for all $a, b \in G$. Is G necessarily abelian?

14. What if the above holds for three consecutive positive integers?

15. If the order of a finite group is even, show that it contains an element $a \neq e$ such that $a^2 = e$.

16. Let G be a group, and let $H \subseteq G$, such that $e \in H$ and $HH \subseteq H$.

    (a) Show that $HH = H$.

    (b) If $|G| < \infty$, show that $H \leq G$.

    (c) Is it enough that $|H| < \infty$?

4 Cyclic groups

1. Judson, section 4.4, exercise 1-2,4,10,12-13,23,30-34,36-37,43-46

2. Svensson, section 4.2, exercise 3-7

3. Svensson, section 4.3, exercise 2,7,12

4. Svensson, section 4.4, exercise 3-4

5. Let T denote the group of complex numbers of unit modulus, under multiplication.

    (a) Find all elements of order 2, order 3, and order 4.

    (b) Find all elements of finite order n.

    (c) Find all finite subgroups of T.

6. Let $\mathbb{C}^*$ be the set of all non-zero complex numbers.

    (a) Show that $\mathbb{C}^*$ is a group under multiplication.

    (b) Call a subroup $H \subseteq C^*$ *bounded* if H is contained in some open disc of finite radius. Show that the circle group $\mathcal{T}$, consisting of complex number of unit modulus, is bounded, and contains all such bounded subgroups.

    (c) A subgroup $K \subset C^*$ is called *discrete* if every open disc of finite radius intersection K in a finite number of points. Show that every such discrete subgroup is in fact bounded. Must it also be cyclic?

    (d) Regard $\mathbb{R}^2$ as an abelian group, with the natural addition. Define the notions of discrete and bounded subgroups as before, mutatis mutandis. Show that the subgroup of $\mathbb{R}^2$ generated by two non-zero, non-parallell vectors yields an example of a discrete, non-bounded subgroup of $\mathbb{R}^2$.

    (e) Show that the cyclic subgroup C generated by a non-zero vector is another such example. Show that the quotient $\mathbb{R}^2/C$ is isomorphic to the cylinder $\mathcal{T} \times \mathbb{R}$.

5 Permutations, Symmetric groups, Symmetry groups

1. Judson, section 5.3, exercise 1,2abgj,3,5-6,11,13,16,23,26,29-30,33,36
2. Svensson, section 5.1, exercise 2,6,8,12,16
3. Svensson, section 5.2, exercise 3,6,8
4. Svensson, section 5.3, exercise 3-4,6
5. If $\sigma = [\sigma(1), \ldots, \sigma(n)]$ is a permutation, then its *set of inversions* is
$$\mathrm{inv}(\sigma) = \{\, (i,j) | i < j, \text{ and } \sigma(i) > \sigma(j) \,\}.$$
   (a) Find $\mathrm{inv}([2,3,1,5,4])$.
   (b) An *adjacent transposition* τ is a transposition that transposes two adjacent integers, i.e., $\tau = (k, k+1)$ for some k. What is $\mathrm{inv}(\tau)$?
   (c) Consider the transposition $\gamma = (k, k+r)$. What is $\mathrm{inv}(\gamma)$? Show that γ can be written as an odd number of adjacent transpositions.
6. Describe the subgroup of S_n generated by all n-cycles.
7. Let X be a finite set with n elements, and let $f \in S_X$. Let σ_1, σ_2 be two bijections from X to $[n]$. Put $\tilde{f}_1 = \sigma_1 f \sigma_1^{-1}$, $\tilde{f}_2 = \sigma_2 f \sigma_2^{-1}$.
   (a) Show that $\tilde{f}_1$ and $\tilde{f}_2$ are conjugate.
   (b) Let $X = \{x, y, z, u, v, w\}$, $f = (x, y, z, u)(v, w)$, $\tilde{f}_1 = (1, 2, 3, 4)(5, 6)$, $\tilde{f}_2 = (1, 3, 6, 4)(2, 5)$. Show that $\tilde{f}_1$ and $\tilde{f}_2$ are conjugate in S_6.
   (c) Show that any two permutations with the same cycle type are conjugate.
8. A permutation $\sigma \in S_n$ with can be written as a product of a_i i-cycles is said to have cycle type $[a_1, a_2, \ldots, a_n]$. How many permutations are there with a given cycle type? What is the order of those permutations? What is the minimal number of tranpositions needed to write such a permutation as a (not necessarily disjoint) product of transpositions?
9. A permutation $\sigma \in S_n$ is an involution if $\sigma = \sigma^{-1}$. Give the possible cycle types of involutions, and count how many involutions there are (for fixed n). Show that any involution can be written as a product of disjoint transpositions.
10. Let $\sigma, \tau \in S_n$ be involutions, such that
$$\sigma = (i_1, i_2)(i_3, i_4) \cdots (i_{r-3}, i_{r-2}), \qquad r < n$$
and
$$\tau = (j_1, i_1)(i_2, i_3)(i_4, i_5) \cdots (i_{r-4}, i_{r-3})(i_{r-2}, j_2), \qquad j_1, j_2 \notin \{i_1, i_2, \ldots, i_{r-2}\}.$$
What is the cycle type of $\sigma\tau$ and $\tau\sigma$? Are they involutions?

11. Find all possible orders of permutations on 5 letters.

12. Let $X = \mathbb{Z}$, and let $G = S_X$. Give an explicit element in G with infinite order.

13. Count the number of permutations in S_n with cycle decomposition consisting of c_1 fixed points, c_2 cycles of length two, and so forth.

14. Let V be a finite set. A simple, undirected graph on V is determined by its edge set $E \subseteq \binom{V}{2}$. A graph isomorphism of $G = (V, E)$ and $H = (W, F)$ is a bijection

$$\phi : V \to W$$

such that

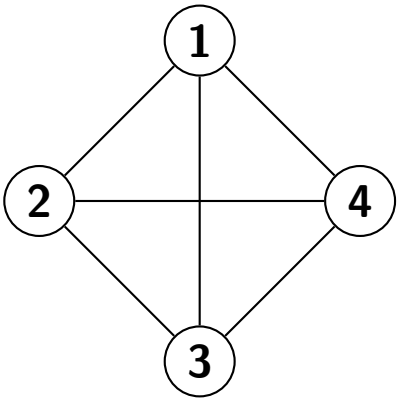
$$\{a, b\} \in E \quad \iff \quad \{\phi(a), \phi(b)\} \in F.$$

A graph automorphism on $G = (V, E)$ is an isomorphism form G to G

(a) Show that the set of automorphisms on G form a group.

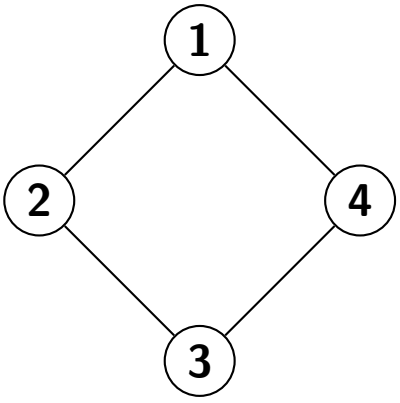
(b) Show that isomorphic graphs have isomorphic automorphism groups.

(c) The complete graph K_n on a vertex set with n elements have an edge between every pair of vertices. The graph K_4 is depicted here.



Determine the automorphism graph of K_4, and more generally for K_n.

(d) Determine the automorphism group of the cycle graph C_4, depicted here:



(e) More generally, the cycle graph C_n on the vertex set $[n]$ has edges

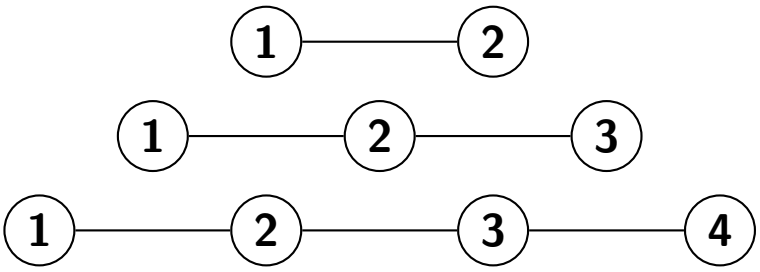
$$\{1,2\},\{2,3\}\ldots\{n-1,n\},\{n,1\}.$$

Determine the automorphism graph of C_n.

(f) The path graph P_n the vertex set $[n]$ has edges

$$\{1,2\},\{2,3\}\ldots\{n-1,n\}.$$

The graphs P_2, P_3 and P_4 are depicted here.



Determine the automorphism graph of P_2, P_3, P_4 and more generally P_n.

(g) Can non-isomorphic graphs have isomorphic automorphism groups?

6 Cosets, Lagrange's theorem

1. Judson, section 6.4, exercise 3-45,8,11,16,18-20
2. Svensson, section 6.1, exercise 2,4,10,15
3. Svensson, section 6.2, exercise 5,7,12
4. Svensson, section 6.3, exercise 2-3,6
5. For a positive integer n, let $U_n = \{\, [m]_n | \gcd(m,n) = 1 \,\}$.
   (a) Show that this is well-defined.
   (b) Show that U_n forms a group under multiplication modulo n.
   (c) Show that U_{13} is cyclic.
   (d) Show that U_9 is cyclic.
   (e) Show that U_8 is not cyclic.
   (f) For which n is U_n cyclic?
6. Suppose that G is a group, A, B are subgroups of G, and that $g \in G$. Show that $gA \cap gB$ is a left coset of $A \cap B$.
7. Suppose that $K \leq H \leq G$ are finite groups. Show , without using Lagrange's theorem, that

$$|G : K| = |G : H| \cdot |H : K|$$

7 Isomorphisms, Cayley's theorem

1. Judson, section 9.3, exercise 1-4,12,14
2. Svensson, section 8.1, exercise 2,4-5
3. Svensson, section 8.2, exercise 1
4. Svensson, section 8.3, exercise 1
5. Let G be the group generated by the permutations $(1,2)$, $(2,3)$, and $(4,5)$.
   (a) List all elements in G
   (b) Is G cyclic?
   (c) Is G abelian?
   (d) Which well-known group is G isomorphic to?

8 Homomorphisms, normal subgroups, quotient groups

1. Judson, section 10.3, exercise 1-2,4-6,8-9,11-14
2. Judson, section 11.3, exercise 2-4,8-10,13-14,17
3. Svensson, section 10.2, exercise 2,4,6-7
4. Svensson, section 10.4, exercise 2,7,11
5. For $a, b \in \mathbb{R}$, define
$$F_{a,b}(t) = at + b$$
Let G consist of all $F_{a,b}$ with $a \neq 0$, under composition. Show that G is a group. What is $F_{a,b} \circ F_{c,d}$? Is G abelian? Let H be the subset of G consisting of all $F_{a,b}$ with rational a, b. Show that H is a subgroup, and determine its left and right cosets. Is H normal in G?
Let $N = \{ F_{1,b} | b \in \mathbb{R} \}$. Show that N is normal in G. Describe the quotient G/N.
6. Let Q be the set $\{\pm E, \pm I, \pm J, \pm K\}$, where
$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & i \\ 0 & i \end{bmatrix}$$
Show that
$$I^2 = J^2 = K^2 = -E, \qquad IJK = -E,$$
nad furthermore that
$$IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J,$$

adn that E and $-E$ commute with all other matrices. Show that Q is a subgroup of the group of all invertible 2×2 complex matrices. Write down its multiplication table.

Show that Q has a single subgroup of order 2. Find all cosets of this subgroup. Is it normal?

Find all subgroups of Q with four elements.

7. Let $g \in G$ have finite order, and let $N \triangleleft G$, N non-trivial and proper. Show that $o(gN) \,|o(g)$. Give an example where $o(gN) = o(g)$, and another where $o(gN)$ is a proper divisor of $o(g)$.

8. Let G be a group, and let $x, y \in G$, with $xy = yx$. Suppose that $o(x) = n < \infty$, $o(y) = m < \infty$. What is $o(xy)$?

9. Suppose that G is a group, and that $A, B \leq G$. Is it true that $AB \leq G$ iff $AB = BA$?

10. If $N \triangleleft G$ and H is a sugroup of G, show that NH is a subgroup of G. Show that $N \cap H$ is a normal subgroup of H.

11. Let H be a subgroup of G. Put

$$N(H) = \left\{ g \in G \middle| gHg^{-1} = H \right\}.$$

    (a) Show that $N(H)$ is a subgroup of G containing H.

    (b) Show that $H \triangleleft N(H)$.

    (c) Show that $N(H)$ is the largest subgroup of G in which H is normal.

    (d) Show that $H \triangleleft G$ if and only if $N(H) = G$.

12. Let G be the group of all 2 by 2 real, overtriangular, invertible matrices, and let N denote the subgroup consisting of those matrices with ones on the diagonal.

    (a) Show that N is normal in G.

    (b) Show that G/N is abelian.

    (c) Let $M \leq G$ be the subgroup consisting of those matrices that have determinant one. Is M normal in G?

    (d) Is N normal in M?

13. Let G be a finite abelian group, and let the positive integer n be relatively prime to $|G|$. Prove that every element $g \in G$ has an n-th root, i.e., that there exists some $x \in G$ with $x^n = g$.

14. Let G be a group, $S \subseteq G$ a subset, and $H = \langle S \rangle$ the subgroup generated by S in G. If $gSg^{-1} \subseteq S$ for all $g \in G$, show that $H \triangleleft G$.

15. Determine subgroups K, H in D_4 such that

$$\{1\} \triangleleft K \triangleleft H \triangleleft D_4, \qquad K \triangleleft D_4$$

with all inclusions proper. Determine D_4/K and $(D_4/K)/(H/K)$.

16. Let G be a group.

    (a) Suppose that $S \subseteq G$ is a subset of G such that $gsg^{-1} \in S$ for all $g \in G$ and all $s \in S$. Show that $\langle S \rangle$, the subgroup generated by S, is normal in G.

    (b) Put $K = \langle \{ xyx^{-1}y^{-1} | x, y \in G \} \rangle$. Show that $K \triangleleft G$.

    (c) Show that G/K is abelian.

    (d) If $N \triangleleft G$ and G/N is abelian, show that $K \subseteq N$.

    (e) If $K \subseteq H \leq G$, show that $H \triangleleft G$.

17. (3p) Let $G \subseteq S_{\mathbb{R}}$ be given by all affine maps $\phi_{a,b}$, $a, b \in \mathbb{R}$, $a \neq 0$, $\phi_{a,b}(x) = ax + b$.

    (a) Show that G is a subgroup. Is it normal?

    (b) Let $N = \{ \phi_{1,b} | b \in \mathbb{R} \}$. Show that $N \triangleleft G$.

    (c) Determine G/N.

18. Let $H = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subset S_4$. Show that H is normal in S_4, and describe S_4/H.

19. The center of a group G is

$$Z(G) = \{ g \in G | gx = xg \text{ for all } x \in G \}.$$

    (a) Show that $Z(G) \leq G$

    (b) Show that $Z(G) \triangleleft G$

    (c) Find $Z(D_n)$

20. Let $\phi : G \to H$ be a group homomorphism, with kernel N and image M.

    (a) Show that the group homomorphism

$$\begin{aligned} C_\infty = \langle g \rangle &\to D_n = \langle r, s | r^n = s^2 = rsrs = 1 \rangle \\ g^k &\mapsto r^k \end{aligned}$$

    can be "factored" through the quotient epimorphism

$$\begin{gathered} C_\infty = \langle g \rangle = \{ g^m | m \in \mathbb{Z} \} \to C_n = \langle h \rangle = \left\{ h^k \middle| 0 \leq k < n \right\} \\ g^k \mapsto h^k \end{gathered}$$

(b) More generally, show that ϕ can be factored as $\phi = \hat{\phi} \circ \pi$, where $\pi : G \to G/N$ is the canonical quotient epimorphism, and $\hat{\phi}$ is injective.

(c) Show that the homomorphism of additive groups

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z} \\ n &\mapsto 2n \end{aligned}$$

can be "factored" through the inclusion homomorphism $2\mathbb{Z} \hookrightarrow \mathbb{Z}$.

(d) Show that ϕ factors as $\phi = j \circ \tilde{\phi}$, where j is the inclusion homomorphism, and $\tilde{\phi}$ is surjective.

(e) Show that the group homomorphism $\mathbb{R} \ni t \mapsto \exp(2\pi i t) \in \mathbb{C}^*$ can be factored as

$$\begin{array}{ccccc} \mathbb{R} & \twoheadrightarrow & \dfrac{\mathbb{R}}{\mathbb{Z}} & \to \mathcal{T} \hookrightarrow & \mathbb{C}^* \\ t & \mapsto & t + \mathbb{Z} & \mapsto \exp(2\pi i t) \mapsto & \exp(2\pi i t) \end{array}$$

where the first homomorphism is surjective, and the last is injective.

(f) Can ϕ be factored as $j \circ \bar{\phi} \circ \pi$, with j injective, π surjective, and $\bar{\phi}$ an isomorphism?

9 Direct products, automorphisms, simple groups

1. Judson, section 9.3, exercise 16-19,23,34-43
2. Svensson, section 8.2, exercise 4-6
3. Judson, section 11.3, exercise 1-12
4. Judson, section 11.3, exercise 2-12
5. Svensson, section 10.3, exercise 2,5
6. Svensson, section 10.5, exercise 1,11
7. (a) If G is a group, then $\mathrm{Aut}(G)$ is the set of all automorphisms on G, i.e. all isomorphisms from G to itself. Show that $\mathrm{Aut}(G)$ is a group under composition of functions.

   (b) If $g \in G$, denote by c_g the map $c_g(x) = gxg^{-1}$. Show that $c_g \in \mathrm{Aut}(G)$.

   (c) Automorphisms of the previous type are called inner, and the set of those are denoted by $\mathrm{Inn}(G)$. Non-inner automorphisms are called outer automorphisms. Show that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Is it always a normal subgroup?

   (d) What are the inner automorphisms of an abelian group?

(e) If G is abelian, show that $g \mapsto g^{-1}$ is an outer automorphism.

(f) Describe the automorphism group of a finite cyclic group. Describe the automorphism group of an infinite cyclic group.

8. Let T be an automorphism on G, and let $g \in G$. Show that $T(g^{-1}) = T(g)^{-1}$. Show that $o(g) = o(T(g))$.

9. Let H be a subgroup of G, and T an automorphism of G. Put

$$T(H) = \{\, T(h) | h \in H \,\}.$$

(a) Show that $T(H)$ is a subgroup of G. Is it always isomorphic to H?

(b) H is a characteristic subgroup of G if $T(H) \subseteq H$ for all automorphisms T. Can the inclusion be strict?

(c) Show that characteristic subgroups are normal. Does the converse necessarily hold?

10. Let G be a finite group, and T and automorphism on G such that $T(x) = x$ if and only if x is the identity.

(a) Show that for any $g \in G$ there is some $x \in G$ such that $g = x^{-1}T(x)$.

(b) If furthermore T^2 is the identity, show that G is abelian.

11. Let $G \subseteq S_6$ consist of all permutations σ such that $i \leq 3 \iff \sigma(i) \leq 3$. Find the cardinality of G and show that it is a subgroup. Then find two proper nontrivial normal subgroups $H, K \triangleleft G$ such that $H \cap K = \{()\}$, $HK = G$, and conclude that $G \simeq H \times K$.

12. (a) Let G be a group, $N \triangleleft G$, $K \leq G$, $N \cap K = \{1\}$, $NK = G$. G is then called the interior semidirect product of N and K. Show that S_3 is the semidirect product of $\langle (123) \rangle$ and $\langle (12) \rangle$.

(b) Show that $\phi : K \ni g \mapsto c_g \in \mathrm{Aut}(K)$ is a group automorphism.

(c) Let $M = N \times K$ as a set, and introduce a multiplication by

$$(n_1, k_1) * (n_2, k_2) = (n_1 \phi(k_1)(n_2), k_1 k_2). \tag{1}$$

Show that this turns M into a group isomorphic to G.

(d) Conversely, Let N, K be groups, and let $\phi : K \to \mathrm{Aut}(K)$ be a homomorphism. Define the exterior semidirect product of N and K to be the set $N \times K$, with the multiplication (**??**). Show that this is the interior semidirect product of two subgroups $\tilde{N}$ and $\tilde{K}$ isomorphic to N and K, respectively.

(e) Show that the dihedral group D_n is the semidirect product of $\langle r \rangle$, the subgroup of rotations and the order two subgroup $\langle s \rangle$, generated by the reflection in the x-axis. (Hint: $srs = r^{-1}$ so c_s is inversion.)

13. Let $\mathbf{T}$ be the set of complex numbers of unit modulus, under multiplication.

    (a) Show that for any positive integer n, $\mathbf{T}$ contains a cyclic subgroup of order n.

    (b) Show that $\mathbf{T}$ contains no subgroup isomorphic $\mathbb{Z}_2 \times \mathbb{Z}_2$.

    (c) Show that for any positive integer n, $\mathbf{T}$ contains a subgroup isomorphic to $\mathbb{Z}^n$.

    (d) Show that $\mathbf{T}$ contains a subgroup isomorphic to a direct sum countably infinite many copies of the infinite cyclic group.

    (e) By studying the map $t \mapsto \exp(2\pi i t)$, show that $\mathbf{T} \simeq \mathbb{R}/\mathbb{Z}$.

    (f) Show that $\mathbf{T}$ is generated by any interval containing 1.

14. Let p be an odd prime number. Show that the set of matrices

$$G = \left\{ \left. \begin{bmatrix} 1 & a & -a & b \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \right| a, b \in \mathbb{Z}_p \right\}$$

    is a finite abelian group (under multiplication). Find which direct product of cyclic groups of prime power order it is isomorphic to.

15. Let $\mathbf{u} = (u_1, u_2)^t$ and $\mathbf{v} = (v_1, v_2)^t$ be two linearly independent vectors in $\mathbb{R}^2$, and let $B = \begin{bmatrix} u_1 & v_1 \\ u_2 & v_2 \end{bmatrix}$. Put $L = \{ a\mathbf{u} + b\mathbf{v} | a, b \in \mathbb{Z} \}$. This is called the lattice spanned by $\mathbf{u}$ and $\mathbf{v}$.

    (a) Show that $L \leq \mathbb{R}^2$, and that $\mathbb{R}^2/L \simeq (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$.

    (b) If $\mathbf{f}, \mathbf{g}$ are two other linearly independent vectors in $\mathbb{R}^2$, with associated lattice M and matrix C, show that $L = M$ if and only if $B = CU$ for some two-by-two matrix U with integral entries, and determinant ± 1.

16. Let G, H, and K be finitely generated abelian groups. Show that if $G \times H \simeq G \times K$, then $H \simeq K$. Give a counterexample to show that this cannot be true in general.

17. Detective Duncan has the following clues to the perpetrator of a particularly heinous crime (fomenting torsionist tendencies):

    (a) The "perp" is a finite abelian group

    (b) The size of the "perp" is 200000

    (c) The maximal order of an element of the "perp" is 200

    Help Duncan narrow down the list of suspects!

18. Let H be a subgroup of a group G. Prove or disprove that the normalizer of H is normal in G.

19. Let G be a group of order p^r, p prime. Prove that G contains a normal subgroup of order p^{r-1}.

10 Group actions, Class equation, Sylow's theorems

1. Judson, section 14.4, exercise 2-10,15,17-18,20-22,24
2. Judson, section 15.3, exercise 2,9,12-13,23
3. Svensson, section 12.1, exercise 1,3,5
4. Svensson, section 12.2, exercise 1,4,12-14
5. Svensson, section 12.3, exercise 6,7,14,19
6. Svensson, section 12.4, exercise 1-2,7,8
7. Let G be a group. Is it always true that for any $g \in G$, g and g^{-1} are conjugate? Is it always true that the subgroup generated by the conjugacy class of g is normal in G?
8. The rigid symmetry group of the cube acts on the set of colorings of the faces of the cube using k colors. Compute the number of non-equivalent colorings. Compute the number of non-equivalent colorings that color the top face using the first color.
9. An ancient device of mysterious origin allows enlightened disciples to mentally communicate any non-negative integer strictly less than 64. Having received the number, the device shivers perceptibly, and some of the originally inert embedded gemstones, arranged symmetrically in an equidistant fashion around the rim of the device, lit up, whereas the remainder of the six gemstones remain dim. It has been known since the dawn of time that the pattern of lit and unlit gemstones represent the binary expansion of the communicated integer (with lit gemstones indicating ones). However, from which gemstone to start the decoding, and whether to proceed in a clockwise or counterclockwise fashion — this is something which varies from occasion to occasion, depending on the sacred constellations of the seven heavens!

   Learned maestros have taken to calling two integers which may, given fortuitious celestal circumstances, produce the same divine *lit-unlit gemstone configuration*, mystically connected. The first task any novice in the order of devotees of the ancient device is given, is to calculate the largest number of pairwise non-mystically connected integers in the prescribed range. Do so!
10. Denote by $\mathrm{cyk}(\sigma)$ the number of cycles in the representation of σ as a product of disjoint cycles (including one-cycles). By counting equivalence classes of functions

$$f : [k] \to [n]$$

   under the equivalence

$$f \sim g \qquad \text{iff exists } \gamma \in S_k : \ f \circ \gamma = g$$

show that

$$\frac{1}{k!}\sum n^{\mathrm{cyk}(\sigma)} = \binom{n+k-1}{k}$$

11. A simple graph on a finite set X is determined by its edge set $E \subseteq \binom{X}{2}$. Two such graphs are isomorphic if there is a permutation $\sigma \in S_X$ such that

$$E_2 = \sigma.E_1 = \{\, \{\sigma(a), \sigma(b)\} | \{a, b\} \in E_1 \,\}.$$

How many isomorphism classes of simple graphs are there, if $|X| = 4$? If $|X| = 5$?

12. We can generalize the concept of a simple graph on X be coloring the edges with k colors. Such a k-colored graph can be described by a map $f : \binom{X}{2} \to [k]$; one of the colors is used to indicate that the potential edge is not present in the graph. To such graphs f, g are ismorphic if there is a $\sigma \in S_X$ such that $f = g \circ \sigma$.

How many isomorphisms classes of k-colored graphs are there on two vertices? On three vertices?

13. Let H be a subgroup of G, and denote by S the set of left cosets.

(a) Show that G acts on S by $g.xH = (gx)H$.

(b) Denote the above bijection on S by τ_g. Show that $g \mapsto \tau_g$ is a homomorphism. What is its kernel?

(c) Describe this map when G is cyclic of order 8, and H is the subgroup of order 2.

(d) Describe this map when G is the dihedral group of order 8, and H is the subgroup of order 2 generated by reflection in the x-axis..

14. How many permutations in S_n are conjugate to the permutation (123)? How many permutations in S_n commute with this permutation?

15. Let $\sigma \in S_n$ have cycle type $[a_1, \ldots, a_n]$, $\sum_j j a_j = n$. How many permutations in S_n commute with σ?

16. Write down the class equation for A_3 and A_4.

17. Let $[5] = \{1, 2, 3, 4, 5\}$, and let $X = \binom{[5]}{3}$, the set of unordered triplets of $[5]$.

(a) S_5 acts naturally on $[5]$. Show that the induced action $\phi.\{a, b, c\} = \{\phi(a), \phi(b), \phi(c)\}$ indeed determines an action of S_5 on X.

(b) Determine the number of orbits of this action.

(c) Let $H = \langle (1, 2, 3, 4, 5) \rangle$ act on X as above. Determine the number of orbits.

(d) Same question for $K = \langle (1, 2) \rangle$.

(e) Solve the above questions for S_4 acting on $\binom{[4]}{2}$ instead.

18. Show that the number of conjugacy classes in a finite group G is given by

$$\frac{1}{|G|}\sum_{g\in G}|C_G(g)|, \qquad C_G(g)=\{\, h\in G|gh=hg\,\}.$$

Determine the number of conjugacy classes in D_8 and D_9.

19. Denote by K the hypercube $K=\{\,(x_1,x_2,x_3,x_4)|0\le x_1,x_2,x_3,x_4\le 1\,\}$, and let $V=\{\,(x_1,x_2,x_3,x_4)|x_1,x_2,x_3,x_4\in\{0,1\}\,\}$ be the set of its vertices. Let $\mathbf{e}_1=(1,0,0,0)$, $\mathbf{e}_2=(0,1,0,0)$, $\mathbf{e}_3=(0,0,1,0)$, $\mathbf{e}_4=(0,0,0,1)$. Let $\Delta=\mathrm{conv}(\mathbf{0},\mathbf{e}_1,\mathbf{e}_1+\mathbf{e}_2,\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3,\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3+\mathbf{e}_4)$.

Let $\sigma\in S_4$ act on K by $\sigma.(x_1,x_2,x_3,x_4)=(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)},x_{\sigma(4)})$.

(a) What are the sizes of the orbits?

(b) Put $\Delta_\sigma=\{\,\sigma.(x_1,x_2,x_3,x_4)|(x_1,x_2,x_3,x_4)\in\Delta\,\}$. Determine the volume of this simplex, and show that

$$K=\cup_{\sigma\in S_4}\Delta_\sigma,$$

with $\Delta_\sigma\cap\Delta_\tau$ a simplex of dimension <4, hence of volume zero, for $\sigma\neq\tau$.

(c) Partial credit if you solve the corresponding questions for $n=3$, even more partial if you look at $n=2$.

20. The dihedral group D_n acts naturally on $[n]=\{1,2,\ldots,n\}$. For $n=4,5,6,7$, find

(a) The stabilizers of each $i\in[n]$, are they all isomorphic?

(b) The fixedpoints of all group elements

(c) The number of ways of coloring a necklace with n beads, using k colors, up to dihedral symmetry.

21. The rotational symmetries of a cube has 24 elements. The group acts on the vertices of the cube.

(a) Show that two rotations by 90 degrees suffice to generate the group

(b) Find all stabilizers and show that they are isomorphic

(c) Calculate the number of inequivalent ways of coloring the vertices using k colors

22. The full symmetry group of the cube (including reflections) has 48 elements

(a) Show that the two rotations by 90 degrees, together with the antipodal map, generates this larger group

(b) Can it be generated by fewer elements?

(c) In how many inequivalent ways can we now color the vertices, using k colors?

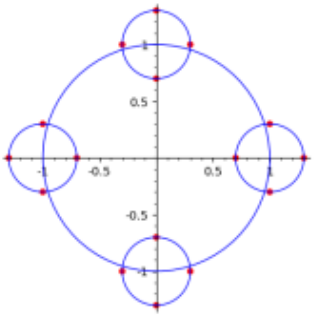
23. Let G be an undirected graph whose vertex set is a subset of $[n]$. Then its edge set is a subset of $\binom{[n]}{2}$. The symmetric group S_n acts on $[n]$, and in a natural way on $\binom{[n]}{2}$, and finally on $\mathcal{P}\left(\binom{[n]}{2}\right)$, thus on the set of all undirected graphs on $[n]$.

(a) How? And why do the orbits correspond to isomorphism classes of graphs?

(b) For $n = 3$, find the number of non-isomorphic graphs, and give a representative from each class. Are there non-isomorphic graphs with the same number of edges?

(c) Do the same for $n = 4, 5$.

24. Consider this arrangement of 16 points:



Enumerate the points using 1,2,3,4 for the rightmost small circle, et cetera. There is a strange group acting on the points, in the following way:

(i) We can rotate the smaller circles on the larger circle, letting the points tag along without turning

(ii) We can rotate all small circle counter-clockwise one quarter turn, then the last three small circles, then the last two, then the last

Call the first operation the "megaturn" and the second operation the "intricate turn". The "strange group" is generated by these, and acts on [16], so we regard it as a subgroup of S_{16}.

(a) What is the size of our strange group? Is it abelian?

(b) Find the stabilizer of point 1. Then express all elements in the stabilizer in terms of intricate and/or mega turns.

(c) In how many inequivalent ways can we color the 16 points, if colorings that can be transformed into each other using intricate and/or mega turns are considered equivalent?

25. (a) Show that the group of complex invertible 2×2 matrices acts on the stereographic one-point compactification of the complex plane by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} .z = \frac{az+b}{cz+d}$$

    (b) What are the orbits?

    (c) What is the fixed point of a general (generic) matrix?

    (d) What is the stabilizer of i?

26. Let G be a finite group of size pm, with p prime, and all prime factors of m larger than p. Suppose that $H \leq G$, $|G : H| = p$. Show that H is normal in G.

    (Hint: G acts on the left cosets of H. This action is equivalent to a homomorphism $G \to S_Y$ for some Y. What is the kernel?)

27. Consider two $m \times n$-matrices A and B as equivalent if by permuting the rows and columns of A we can obtain B. Suppose that the matrices are binary, i.e. have entries in $\{0, 1\}$.

    - Count the number of equivalent binary 2×3-matrices with k ones, for $0 \leq k \leq 6$.
    - Count the number of equivalent binary 3×4-matrices with k ones, for $0 \leq k \leq 12$.
    - Generalize!

11 Rings, definitions, examples, elementary properties

1. Judson, section 16.16, exercise 1,2,4ac,7,9,11,18,24,25,27,34,38,40
2. Svensson, section 13.1, exercise 5,10,12,13,15,16
3. Svensson, section 13.2, exercise 2,3
4. Svensson, section 13.3, exercise 1
5. Svensson, section 14.1, exercise 1,4,6,9,12
6. Svensson, section 14.2, exercise 4
7. Svensson, section 14.4, exercise 4
8. Determine the ideals in $\mathbb{Z} \times \mathbb{Z}$.

9. Let R be a commutative, unitary ring, and I an ideal in R. Suppose that all elements outside I are invertible. Show that I is the unique maximal ideal in R.

10. Let $\mathbb{Z}[i] = \{ a + ib | a, b \in \mathbb{Z} \} \subseteq \mathbb{C}$ be the ring of Gaussian integers. Let $z = 1 + i \in \mathbb{Z}[i]$, and let $I = (z)$. Show that I is a maximal ideal, and that $\mathbb{Z}[i]/I$ is a field with two elements.

11. Let R denote the set of all subsets of S_3. Introduce the addition $A + B = A \Delta B$ (symmetric difference) and multiplication

$$A * B = \{ \sigma \in S_3 | ab = \sigma,\ a \in A,\ b \in B \text{ has an odd number of solutions} \}.$$

    (a) Show that R becomes a ring.

    (b) Show, by an example, that R is not commutative, nor a field.

    (c) Calculate

$$\{(), (1,2), (1,2,3)\} * \{(1,3), (2,3)\}$$

    (d) Let $u = \{(2,3), (1,2), (1,3)\}$, and put $v = u^2$. Show that v is a central idempotent, i.e., $v^2 = v$ and v commutes with everything.

12. For $2 \leq n \leq 20$, check whether $U_n = Z_n^\times$ is cyclic. Formulate a bold hypothesis.

13. Let R be a commutative, unitary ring. Let

$$\mathrm{Nil}(R) = \{ r \in R | \exists n \geq 1,\ r^n = 0 \}.$$

    (a) Show that $\mathrm{Nil}(R)$ is an ideal of R.

    (b) Show that $\mathrm{Nil}(R)$ is not necessarily an ideal of a non-commutative ring R.

    (c) Show that if $r \in \mathrm{Nil}(R)$ then $1 - r$ is invertible in R.

14. Find the characteristic of the following commutative rings:

    (a) $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}} \times \frac{\mathbb{Z}}{15\mathbb{Z}}$

    (b) $\mathbb{Z}[i]$, where $i \in \mathbb{C}$, $i^2 = -1$

    (c) $\frac{\mathbb{Z}[j]}{(2-5j)}$ where j is a primitive 3rd root of unity, $j^3 = 1$ but, $j^2 \neq 1$, you can explicitly take $j = \exp(\frac{2}{3}\pi i) \in \mathbb{C}$.

15. Provide explicit ring isomorphisms between

    (a) $\frac{\mathbb{Z}[x]}{(n,x)}$ and $\frac{\mathbb{Z}}{n\mathbb{Z}}$,

    (b) $\frac{\mathbb{Z}[x]}{(n)}$ and $(\frac{\mathbb{Z}}{n\mathbb{Z}})[x]$.

16. Which of the following ideals in $\mathbb{Z}[x]$ are prime? Which are maximal?

    (a) $(x, x+1)$,

    (b) $(5, x^2+4)$,

    (c) $(x^2+1, x+2)$.

12 Polynomial rings

1. Judson, section 17.4, exercise 2e,3a,4a,5b,6,7,11,18,19,20,24,25
2. Svensson, section 16.1, exercise 5,8
3. Svensson, section 16.2, exercise 4,5
4. Svensson, section 16.3, exercise 2,4
5. Svensson, section 16.4, exercise 1,4
6. Svensson, section 16.5, exercise 3,5
7. Svensson, section 16.6, exercise 2,6
8. Does $f(x) = 2x + 1 \in \mathbb{Z}_4[x]$ have a multiplicative inverse?
9. Let $f(x) = x^2 + x + 1 \in \mathbb{Q}[x]$, $I = (f(x))$, $R = \mathbb{Q}[x]/I$. For each positive integer n, determine $x^n + I$. Use this to show that $f(x) \,|(x^n + x + 1)$ iff $n \equiv 2 \mod 3$.
10. Let K be a field, and let $R = K[x]$. If $f(x) = \sum_{j=0}^{n} a_j x^j \in R$, define the formal derivative of $f(x)$ as $f'(x) = \sum_{j=1}^{n} a_j j x^{j-1}$.
    (i) Show that $f(x) \mapsto f'(x)$ is K-linear.
    (ii) Show that $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.
    (iii) Can we extend the definition of formal derivatives to the fraction field $K(x)$, in such a way that the above properties still hold?
    (iv) (1p) Call the sum $f_e(x) = \sum_j a_{2j} x^{2j}$ the *even part* of $f(x)$. Show that when $\mathrm{char}(K) \neq 2$,
    $$f_e(x) = \frac{1}{2} f(x) + \frac{1}{2} f(-x).$$
    (v) When $\mathrm{char}(K) = 2$, what can you say about $f_e'(x)$?
    (vi) If $f(x) = g(x)^a h(x)^b$ with $g(x), h(x)$ irreducible and relatively prime, calculate $\gcd(f(x), f'(x))$ and $\frac{f(x)}{\gcd(f(x), f'(x))}$
    (vii) In particular, calculate the latter quantity when
    $$f(x) = (1 - x^2 + x^3 - x^5)(x^3 + 2) \in \mathbb{Z}_3[x]$$
    Note: needs no computer!
11. Let $R = \mathbb{Q}[D_4]$, the group algebra on $D_4 = \langle r, s | r^4 = s^2 = rsrs = 1 \rangle$. In other words, R is the $\mathbb{Q}$-vector space with basis elements labeled with the elements of D_4, and with multiplication the $\mathbb{Q}$-linear extension of the multiplication on basis elements given by the multiplication of D_4.

(a) Put $t = 1 * r + 1 * s \in R$. Calculate $t * t$ and $t * t * t$

(b) Put $v = 1 * 1 + 1 * s$. Find an explicit expression for v^k for any positive k.

(c) Show that the map

$$F : \mathbb{Q}[D_4] \to \mathbb{Q}$$
$$\sum_{g \in D_4} c(g)g \mapsto \sum_{g \in D_4} c(g)$$

is $\mathbb{Q}$-linear and calculate its kernel.

(d) Show that the *left annihilator*

$$\mathrm{Ann}(t) = \{\, f \in R | f * t = 0 \,\}$$

is a left ideal of R, and calculate a basis of it as a $\mathbb{Q}$-vector space.

(e) List the conjugacy classes in D_4. Calculate the *center* of R, i.e.,

$$\mathrm{Center}(R) = \{\, f \in R | f * h = h * f \text{ for all } h \in R \,\}$$

Compare.

13 Monomial ideals

1. Let $R = \mathbb{C}[x, y]$ and let $M = \{\, (a, b) \in \mathbb{Z}^2 | a, b \geq 0 \,\}$. Then R is a commutative, unitary ring, and M is a monoid under componentwise addition. Put $X = \left\{\, x^a y^b \middle| a, b \in \mathbb{Z}, a, b \geq 0 \,\right\}$. Then X is a $\mathbb{C}$-basis for R. For $f \in R$, we write

$$f = \sum_{(a,b) \in M} c_{a,b} x^a y^b = \sum_{x^a y^b \in X} c_{a,b} x^a y^b,$$

and put $\mathrm{supp}(f) = \{\, (a, b) \in M | c_{a,b} \neq 0 \,\}$. Note that this set is finite.

(a) We say that an ideal $I \subseteq R$ is a monomial ideal if

$$f \in I \implies x^a y^b \in I \text{ for all } (a, b) \in \mathrm{Supp}(f).$$

Show that an ideal is a monomial ideal if and only if it is generated by monomials.

(b) A subset $J \subset M$ is called a monoid ideal if $(a, b) \in J \implies (a, b) + (c, d) \in J$ for all $(c, d) \in M$. Show that the exponential mapping

$$M \ni (a, b) \mapsto x^a y^b \in X \subset R$$

induces a bijection between the set of monomial ideals in R and the set of monoid ideals in M.

(c) Show that, under this bijection, union of monoid ideals (which is again a monoid ideal) correspond to sums of monomial ideals. Show furthermore that intersections correspond to intersections.

(d) Draw a figure (by shading lattice points in the positive quadrant) of $I = (x^2, y^3)$ and of I^2, and of $J = (x^2, xy)$. Calculate (i.e. give generators for) $I^2 + J$, $I^2 \cap J$ and $I^2 J$.

(e) For all the above ideals, the quotient ring is a vector space over $\mathbb{C}$. Give vector space bases for these spaces!

(f) Show that if $I \subset \mathbb{Q}[x, y]$ is a monomial ideal, then both $I \cap \mathbb{Q}[x]$ and $I \cap \mathbb{Q}[y]$ are ideals, the so-called *elimination ideals*. Show furthermore that these ideals are either the zero ideal, or generated by a power of the indeterminate.

(g) If both elimination ideals are non-zero, show that the quotient ring

$$\frac{\mathbb{Q}[x, y]}{I}$$

has finite dimension as a $\mathbb{Q}$-vector space.

(h) Describe the radical monomial ideals in this ring.

(i) Describe the maximal monomial ideals in this ring.

14 Power series rings

1. Let R be a commutative, unitary ring, and I an ideal in R. Suppose that all elements outside I are invertible. Show that I is the unique maximal ideal in R.

2. Let $R = \mathbb{C}[[t]]$, the ring of formal power series in t with complex coefficients.

   (a) By inductively solving an infinite system of equations, show that $\sum_{\ell \geq 0} a_\ell t^\ell$ is invertible iff $a_0 \neq 0$. Conclude that (t) is the unique maximal ideal in R.

   (b) Show that any $f \in R$ (should be non-zero f) can be uniquely written as a product $f = ut^m$, where m is a non-negative integer and $u \in R$ is a unit.

   (c) List all ideals in R.

   (d) We say that $f_n \to f \in R$ as $n \to \infty$ if, for all m, there is some $N(m)$ so that $n > N(m)$ implies that $f - f_n \in (t)^m = (t^m)$. Take any $f \in R \setminus (t)$ and write it as $c(1 - g)$ with $g \in (t)$. Show that $(1 - g)(1 + g + g^2 + \cdots + g^n) \to 1$ as $n \to \infty$. Hence, the inverse of $1 - g$ is $\sum_{\ell \geq 0} g^\ell$, and the inverse of f is $c^{-1} \sum_{\ell \geq 0} g^\ell$.

15 Factorization in domains

1. Judson, section 18.3, exercise 4,9,10,11abc,12,14,15,20

2. Svensson, section 17.1, exercise 3

3. Svensson, section 17.2, exercise 1ad,2ad,10ac,13ab

4. Svensson, section 17.4, exercise 4ab,5a,8a,12

16 Quotients of rings

1. Consider the complex square matrix

$$C = \begin{bmatrix} 3 & 1 & 1 & 1 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

   Find the characteristic polynomial of C. Calculate C^2, and show that the set $\{I, C, C^2\}$ is linearly dependent. Use this to show that the minimal polynomial has degree 2, and calculate it.

   Let R be the $\mathbb{C}$-algebra generated by C. Show that is isomorphic to $\mathbb{C}[x]/(x^2)$.

2. Let $A \in M_n(\mathbb{C})$, the C-algebra of n-by-n complex matrices.

   (a) Show that there exists a $\mathbb{C}$-sub-algebra S of $M_n(\mathbb{C})$ that is smallest among those that contain A. Show furthermore that S is commutative, and that it is of finite vector space dimension. Is it always a domain?

   (b) Show that for a polynomial $p(t) \in \mathbb{C}[t]$, $p(A) \in S \subseteq M_n(\mathbb{C})$. Show furthermore that the map

$$\mathbb{C}[t] \ni f(t) \mapsto f(A) \in S$$

   is a surjective $\mathbb{C}$-algebra homomorphism.

   (c) Denote the kernel of this map by $I = (g)$. The polynomial g is called the minimal polynomial of A. Show that g divides any polynomial $h(t)$ for which $h(A) = 0$. Is g necessarily irreducible?

   (d) Let

$$A = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & 1 & 0 \end{bmatrix}.$$

   Calculate the characteristic polynomial $p(t) = \det(tI - A)$, and evaluate it at A. Factor $p(t)$, then try to find the minimal polynomial of A.

3. Let $g(x) = x^6 - x^3 - 2 \in \mathbb{Q}[x]$. Put $R = \mathbb{Q}[x]/(g(x))$.

(a) Is R an integral domain?

(b) Find all proper, non-trivial ideals of R.

(c) Let a denote the coset $x + (g(x)) \in R$. Find, if possible, the inverse of a.

(d) Find a general expression for a^k, $k \geq 0$, as a linear combination of $a^0, a^1, a^2, a^3, a^4, a^5$.

17 Fields and field extensions

1. Judson, section 21.4, exercise 1,2a-f,3abc,5,9,12,15,22,26,28
2. Svensson, section 18.1, exercise 5
3. Svensson, section 18.2, exercise 2,3,6,10,15,23,26
4. Svensson, section 18.3, exercise 1,2,11,14
5. Svensson, section 20.1, exercise 2,6,8,14,17
6. Svensson, section 20.2, exercise 3,4,6
7. Find the splitting fields for the following rational polynomials. Give the dimensions, as well as vector space bases, as well as primitive element for the extension.

   (a) $x^3 - 11$,

   (b) $x^4 + x^2 + 1$.

8. The element $\gamma \in \mathbb{C}$ has minimal polynomial $t^3 + t + 1$ over $\mathbb{Q}$. What is the minimal polynomial of $\gamma + \sqrt{2}$ over $\mathbb{Q}$?
9. Let $\alpha = \sqrt{3} + i \in \mathbb{C}$. Determine the minimal polynomial of α over

   (a) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$,

   (b) $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{3}, i)$.

10. Determine the degrees of the splitting fields of the following polynomials with rational coefficients.

    (a) $x^4 + x^3 + x + 1$,

    (b) $x^4 + x^3 + x^2 + x + 1$,

    (c) $x^4 - 8x^2 + 8$,

    (d) $x^4 - 6x^2 + 2$,

    (e) $x^4 + x^3 + x^2 + x + 2$.

11. Find the splitting fields of the following polynomials, and calculate the degree of the extension. Prove your assertions meticulously!

(i) $x^4 + 4 \in \mathbb{Q}[x]$,

(ii) $x^3 - 5 \in \mathbb{Q}[x]$,

(iii) $x^5 - 1 \in \mathbb{Q}[x]$,

(iv) $x^5 - 2 \in \mathbb{Q}[x]$,

(v) $x^4 - 8x^2 + 8 \in \mathbb{Q}[x]$,

(vi) $x^4 - 6x^2 + 2 \in \mathbb{Q}[x]$,

(vii) $x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$,

(viii) $x^3 - y \in \mathbb{Z}_3(y)[x]$, (the coefficient field is the field of rational functions)

12. Find $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{2}, i\sqrt{3})$. What is the minimal polynomial of α over $\mathbb{Q}$?

13. Let p be a prime number, and let $f(x) = x^p - x \in \mathbb{Z}_p[x]$. Factor $f(x)$ into irreducible factors.

14. Let $\alpha = \sqrt{2} + \sqrt[3]{5}$. Find the minimal polynomial of α over $\mathbb{Q}$ and the degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

15. Let $\alpha \in \mathbb{C}$. Then α is an algebraic integer iff it is the root of an equation of the form

$$\alpha^m + b_1\alpha^{m-1} + \cdots + b_m = 0, \qquad b_1, \ldots, b_m \in \mathbb{Z}$$

    (a) Show that an algebraic integer is algebraic over $\mathbb{Q}$.

    (b) Show that the converse does not hold.

    (c) Show that any element of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$ can be scaled by a positive integer to become an algebraic integer.

    (d) Show that $\sqrt{1/3} + \sqrt[3]{1/5}$ is not an algebraic integer; scale it with a positive integer so that it becomes one.

16. (4p) Recall that a field isomorphism is a ring isomorphism preserving the multiplicative identity, and that a field automorphism is a field isomorphism from the field to itself.

    (a) Prove that complex conjugation is a field automorphism.

    (b) What are the field automorphisms of $\mathbb{Q}$?

    (c) What are the field automorphisms of $\mathbb{Q}(\sqrt[3]{2})$?

    (d) What are the field automorphisms of a field with 27 elements?

17. Let $\alpha \in \mathbb{C}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Put $\beta = \alpha^3$.

    (a) What is $[\mathbb{Q}(\beta) : \mathbb{Q}]$?

    (b) If $\alpha^5 = \alpha - 1$, what is the minimal polynomial of β?

18 Finite fields

1. Judson, section 22.3, exercise 1ab,2,3,5,6,7,12,14,16,20,21,22,23,24
2. Svensson, section 20.3, exercise 1,5,7,11
3. Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$, $g(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.
   (a) Show that $E_1 = \mathbb{Z}_2[x]/(f(x))$ is a field, and find an inverse to $x + 1 + (f(x))$.
   (b) Show that $E_2 = \mathbb{Z}_2[x]/(g(x))$ is a field, and find all generators to its multiplicative group.
   (c) Show that $\mathbb{Z}_2[x]/(f(x)g(x))$ is isomorphic to the product of two fields.
   (d) Find the splitting fields of $f(x)$ and of $g(x)$.
   (e) Find the splitting fields of $f(x)g(x)$.
4. Consider the recurrence equation

$$s_t + s_{t-3} + s_{t-5} = 0, \qquad s_0 = 1, s_1 = 0, s_2 = 0, s_3 = 0, s_4 = 0 \in \mathbb{Z}_2.$$

   Let $f(x) = x^5 + x^2 + 1$, and let $g(x) = \frac{1}{x^5} f(x)$.
   (a) Show that $f(x)$ and $g(x)$ are irreducible.
   (b) Put $R_1 = \mathbb{Z}_2[x]/(f(x))$ and $R_2 = \mathbb{Z}_2[x]/(g(x))$. Denote by ϕ_1 the linear map on R_1 given by multiplication with the image of x. Determine its matrix A_1 w.r.t. the basis $[1, x, x^2, x^3, x^4]$, and calculate the smallest n_1 such that $A_1^{n_1} = I$. Use this to determine the order of the image of x in the multiplicative group of R_1. Do the same for g.
   (c) Calculate the smallest positive integer m_1 such that $x^m - 1$ is divisible by $f(x)$.
   (d) Give an explicit formula for c_j for all $j \geq 0$.
5. What is the probability that a randomly choosen $n \times n$ matrix with entries in $GF(p^n)$ is invertible?
6. (7p) Solve the reccurence equation

$$a_n = a_{n-1} + a_{n-2} \in \mathbb{Z}_3$$

   with initial conditions $a_0 = a_1 = 1$, in the following way:
   (i) Show that $f(x) = x^2 - x - 1 \in \mathbb{Z}_3[x]$ is irreducible, as is $g(x) = x^2 + x - 1 \in \mathbb{Z}_3[x]$
   (ii) Define $p(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Z}_3[[x]]$.
   (iii) Show that (in $\mathbb{Z}_3[[x]]$),

$$\sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} a_{n-2} x^n$$

(iv) Turn this into an equation for $p(x)$

(v) Solve for $p(x)$. You should get a rational function.

(vi) Let E be the splitting field of $f(x)$, or of $g(x)$, whatever you find convenient. Perform partial fraction decomposition of $p(x)$ in E.

(vii) Prove that the geometric formula

$$\frac{1}{1-ux} = 1 + u^2x^2 + u^3x^3 + u^4x^4 + \dots$$

holds for any $u \in E \setminus 0$, and use this to find an explicit formula for a_n.

7. (6p) Let $F = GF(9)$, expressed as $\mathbb{Z}_3[y]/(y^2+2y+2) \simeq \mathbb{Z}_3(a)$.

(a) There are of course 9 irreducible monic linear polynomials in $F[x]$; how many irreducible quadratic polynomials are there?

(b) The following sequence of elements in F is periodic; enough of it is given that you will be able to deduce the period.

$$(c_j)_{j=0}^{\infty} = (2*a+1, 1, 2, 2*a+2, 2, 2*a, 0, a+1, a+1, 2*a, 2, a, 2*a,$$
$$a+2, 2*a, 2*a+2, 0, 2*a+1, 2*a+1, 2*a+2, 2*a, a+1, 2*a+2, 1, 2*a+2, a+2,$$
$$0, 2, 2, a+2, 2*a+2, 2*a+1, a+2, a, a+2, 1, 0, 2*a, 2*a,$$
$$1, a+2, 2, 1, a+1, 1, a, 0, 2*a+2, 2*a+2, a, 1, 2*a, a, 2*a+1,$$
$$a, a+1, 0, a+2, a+2, a+1, a, 2*a+2, a+1, 2, a+1, 2*a+1, 0, 1, 1, 2*a+1,$$
$$a+1, a+2, 2*a+1, 2*a, 2*a+1, 2, 0, a, a, 2, 2*a+1, 1, 2, 2*a+2, 2, 2*a,$$
$$0, a+1, a+1, 2*a, 2, a, 2*a, a+2, 2*a, 2*a+2, 0, 2*a+1, 2*a+1, 2*a+2, 2*a, a+1, 2*a+2,$$
$$1, 2*a+2, a+2, 0, 2, 2, a+2, 2*a+2, 2*a+1, a+2, a, a+2, 1, 0, 2*a, 2*a, 1, \dots)$$

Find this period (and preperiod, if applicable).

(c) Find the recurrence relation over F that this sequence satisfies.

(d) Find the generating function of the sequence.

(e) Factor the denominator of the generating function (over some explicit extension of F), then perform partial fraction decomposition of the generating function.

(f) Find an explicit formula for c_j of the form

$$c_j = u\alpha^j + v\beta^j$$

where u, v, α, β lies in some (explicit) extension of F.

8. Let F be a field with $q < \infty$ elements, and let K be an extension of F.

(a) Prove that $a^q = a$ for all $a \in F$.

(b) If $b \in K$ is algebraic over F, show that $b^{(q^m)} = b$ for some $m > 0$.