

The Important Theorems
Mathematics 309a Abstract Algebra
Winter Semester 2008
David Haines

From: Fraleigh, John B. *A First Course in Abstract Algebra*. 7th ed. Addison-Wesley. 2003.

Section 2 Binary Operations

2.15. Composition of Functions is Associative

Section 3 Isomorphic Binary Structures

3.13. There is at Most One Identity Element in Any Binary Structure

3.14. Isomorphisms Preserve Identity Elements

Section 4 Groups

4.15. Both Cancellation Laws Hold in Groups

4.16. Linear Equations Have Unique Solutions in Groups

4.17. Uniqueness of the Identity Element and Inverses in a Group

4.18. The Inverse of a Product is the Product of Inverses in the Reverse Order

Section 5 Subgroups

5.14. Simplified Criteria for a Subgroup

5.17. How to Construct the Smallest Subgroup Containing a Given Element

Section 6 Cyclic Groups

6.1. Every Cyclic Group is Abelian

6.6. Every Subgroup of a Cyclic Group is Cyclic

6.10. A Classification Theorem for Cyclic Groups

6.14. How to Construct a Subgroup of a Cyclic Group

Section 7 Generating Sets and Cayley Digraphs

7.4. The Intersection of Subgroups is a Subgroup

7.6. How to Construct a Subgroup from Generators

Section 8 Groups of Permutations

8.5. The Permutations of a Set Are a Group under Permutation Multiplication

8.16. (Cayley) Every Group is Isomorphic to a Group of Permutations

Section 9 Orbits, Cycles, and the Alternating Groups

9.8. Any Permutation in S_n is a Product of Disjoint Cycles

9.12. If $n > 1$, Any Permutation in S_n is a Product of Transpositions

9.15. No Permutation in S_n Can Be Both Even and Odd

9.20. If $n > 1$, Half of the Permutations in S_n Are Even and Form a Subgroup of S_n

Section 10 Cosets and the Theorem of Lagrange

10.1. Every Subgroup Determines an Equivalence Relation on the Group that Contains It

- 10.10. (Lagrange) The Order of a Subgroup Divides the Order of the Group that Contains It
- 10.11. Every Group of Prime Order Is Cyclic
- 10.12. The Order of an Element in a Finite Group Divides the Order of the Group
- 10.14. Concerning the Index of a Subgroup of Subgroup of a Group

Section 11 Direct Products and Finitely Generated Abelian Groups

- 11.2. How to Use the Cartesian Product to Construct a New Group from Other Groups
- 11.5. For Which Cyclic Groups is their Product Cyclic?
- 11.9. How to Compute the Order of Any Element in a Product of Groups
- 11.12. The Fundamental Theorem of Finitely-Generated Abelian Groups
- 11.15. Classification of the Finite Indecomposable Abelian Groups
- 11.16. A Way to Find Subgroups of Finite Abelian Groups
- 11.17. Any Abelian Group of Square Free Order is Cyclic

Section 13 Homomorphisms

- 13.12. A Group Homomorphism Preserves Identities, Inverses, and Subgroups
- 13.15. Left and Right Cosets of Kernels Coincide
- 13.18. A Group Homomorphism is One-to-One If and Only If Its Kernel Is Trivial
- 13.20. Kernels Are Normal Subgroups

Section 14 Factor Groups

- 14.1. How to Construct Factor Groups from Kernels
- 14.4. Left Cosets with Coset Multiplication Are a Group If and Only If the Cosets Come from a Normal Subgroup
- 14.9. How to Construct a New Homomorphism by Sending Elements to those Cosets of a Normal Subgroup that Contain Them.
- 14.11. The Fundamental Homomorphism Theorem
- 14.13. Three Ways to Tell If a Subgroup is Normal

Section 15 Factor-Group Computations and Simple Groups

- 15.6. The Converse of Lagrange's Theorem is False
- 15.8. Finding a Normal Subgroup within a Product of Two Groups and How to Determine Its Factor Group
- 15.9. Factor Groups of Cyclic Groups are Cyclic
- 15.16. Group Homomorphisms Preserve Normal Subgroups
- 15.18. A Subgroup is a Maximal Normal Subgroup If and Only If Its Factor Group is Simple
- 15.20. The Commutator Subgroup is Normal, Its Factor Group is Abelian, and Even More.

Section 18 Rings and Fields

- 18.8. In Any Ring, 0 and Negation Work in the Familiar Ways

Section 19 Integral Domains

- 19.3. Determining Those Elements of \mathbb{Z}_n Which Divide Zero
- 19.4. If p Is Prime, \mathbb{Z}_p Has No Divisors of Zero
- 19.5. The Cancellation Laws Hold in a Ring If and Only If the Ring Has No Divisors of 0
- 19.9. Every Field is an Integral Domain
- 19.11. Every Finite Integral Domain is a Field

- 19.12. If p Is Prime, \mathbb{Z}_p is a Field
19.15. How to Determine the Characteristic of a Ring

Section 20 Fermat's and Euler's Theorems

- 20.1. Fermat's Little Theorem
20.6. The Elements of \mathbb{Z}_n Which are Not Zero Divisors Form a Group under Multiplication Modulo n
20.8. Euler's Theorem
20.10. A Condition to Assure that $ax = b$ has a Unique Solution in \mathbb{Z}_n
20.11. A Condition to Allow the Discovery of All Integer Solutions to $ax \equiv b \pmod{m}$
20.12. Finding All Solutions to the Linear Equation $ax = b$ in \mathbb{Z}_n
20.13. Finding All Integer Solutions to $ax \equiv b \pmod{m}$

Section 21 The Field of Quotients of an Integral Domain

- 21.5. Any Integral Domain Can Be Enlarged to a Field in Such a Way that Every Element of the Field Can Be Expressed as the Quotient of Two Elements in the Integral Domain
21.6. The Field of Quotients of an Integral Domain is the "Smallest" Field Containing that Integral Domain

Section 22 Rings of Polynomials

- 22.2. The Polynomials with Coefficients in a Ring Themselves Form a Ring Under Polynomial Arithmetic.
22.4. The Evaluation Homomorphisms for Field Theory
22.11. $x^2 - 2$ Has No Zeros in the Rational Numbers

Section 23 Factorization of Polynomials over a Field

- 23.1. The Division Algorithm for Polynomials
23.3. The Factor Theorem
23.5. Any Nonzero Polynomial of Degree n Over a Field Has At Most n Zeros in that Field
23.6. Any Finite Subgroup of the Multiplicative Group of a Field is a Cyclic Group
23.10. A Polynomial of Degree 2 or 3 Over a Field Is Reducible If and Only If It Has a Zero in the Field
23.11. A Polynomial with Integer Coefficients Factors Over the Rational Polynomials If and Only If It Factors into Polynomials with Integer Coefficients.
23.12. Any Monic Polynomial with Integer Coefficients and Non-zero Constant Term Which Has a Zero in the Rationals Also Has a Zero in the Integers and That Zero Divides Its Constant Term
23.15. Eisenstein Criterion for Irreducibility
23.17. The Cyclotomic Polynomial of Prime Degree is Irreducible over the Rationals
23.18. If an Irreducible Polynomial Divides the Product of Two Polynomials, Then It Divides at Least One of the Polynomials
23.20. Every Non-Constant Polynomial Over a Field Can Be Factored Into a Product of Irreducible Polynomials in an Essentially Unique Way