361 Honors Algebra III, Fall 1996
A. Goetz

Textbook: Abstract Algebra by I. N. Herstein, Third Edition.

Syllabus

1. Elements of set theory.
Definition: set, subset, union, intersection, difference (relative complement), empty set, universe, complement. Venn diagrams. Associative, commutative and distributive laws for union and intersection. De'Morgan laws. Symmetric difference and its properties (to be used later as an example of a ring of characteristic 2). (Chapter 1, Section 2)

2. Mappings.
Injective, surjective and bijective mappings. Composition of mappings. The associative property of the composition of mappings. (Chapter 2, Section 3) Permutations of a set A. Identity mapping, inverse mapping. Group properties of permutations (Chapter 2, Section 4) S_n . Cycles, disjoint cycle decomposition of a permutation. Transpositions, and the representation of a permutation as a product of transpositions. Even and odd permutations. Representation of every even permutation as a composition of 3-cycles. (Chapter 3, Sections 1-3)

3. Rudiments of number theory.
Arithmetical properties of integers. The principle of mathematical induction, the well ordering principle. Division with remainder. Divisibility. The greatest common divisor of two numbers. Euclid's algorithm. Relatively prime numbers.
(Chapter 1, Sections 5-6)
Congruences modulo n. Definition properties. Addition and multiplication of congruences. Cancellation laws: $ab = ac \pmod{n}$ is equivalent to $b = c \pmod{n}$, if $(a, n)= 1$, $ab = ac \pmod{an}$ is equivalent to $b = c \pmod{n}$ for any $a \ne 0$. Solutions of a Diophantine equation. Solutions of a congruence $ax \equiv b \pmod{n}$, and of a system of congruences of first degree. Equivalence relations and equivalence classes. Equivalence classes modulo n. Arithmetic of Z_n. Invertible elements and zero divisors in Z_n . (The textbook introduces congruences modulo n as examples in Section 2.4 and deals with them through problems to this section)

4. Complex numbers.
Definition. Addition and multiplication, complex conjugate, modulus, inverse. Polar form, argument, multiplication in polar form. De'Moivre's theorem, n-th roots of a complex number. n-th root of

unity, primitive roots. (Chapter 2, Section 7)

5. Group theory.
Definitions: Group, Abelian group, subgroup. Examples of groups: Previously encountered: Z, Z_n, Q, R, C, rectangular matrices with addition, Q^+, R^+, C-{0}, nonsingular square matrices, S_n and various groups of transformations, the power set of a non empty set with symmetric difference. Newly introduced: U_n, the set of all invertible elements of Z_n with multiplication, dihedral groups. The 4 group and the quaternion group (Chapter 1, Section 1)

Some elementary properties of groups: uniqueness of identity element and inverses. Cancellation law etc. (Chapter 2, Section 2) Cyclic groups. Order of a group, order of an element. Cyclic subgroups, cyclic groups (Chapter 2. Section 3)

Right and left cosets. Lagrange's theorem and some simple consequences, e. g. every group of prime order is cyclic, for every a in G, a^{o(G)} = e. Index if a subgroup. Euler's and Fermat's theorems (Chapter 2, Section 4)

Isomorphisms of groups. Examples: Dihedral group of order 6 and S do5(3), Square 2x2 matrices of form \pmatrix{a&b\cr-b&a\cr} and complex numbers and many others. Isomorphism of cyclic groups. Automorphisms. Inner automorphisms. Cayley's theorem.

Homomorphisms of groups. Kernel of an homomorphisms. One to one homomorphisms homomorphisms onto. Normal subgroups. Counter example for transitivity of the normal subgroup relation. Every right cosets of a subgroup is a left coset if and only if the subgroup is normal. (Chapter 2, section 5)

Factor groups. The natural homomorphism G \to G/N. Examples of factor groups. Order of the factor group. Cauchy's theorem for Abelian groups. (Chapter 2, section 6) The first second and third homomorphism theorems, the correspondence theorem. (Chapter 2, Section 7)

Direct products of groups (Chapter 2, Section 9) Representation of an Abelian group as a direct product of p-groups. (Chapter 2, Section 10)

Conjugacy. Conjugacy in S_n. Proof that S_5 is a simple group. Conjugacy classes and the class equation. Sylow's theorem. (The proof of the first theorem given in class. Assigned homework (Problems 27 and 28 on p. 107) was leading to a proof of the second theorem.

Students had difficulty with these problems and I have to discuss them in class). (Chapter 2, Section 11) Definitions of a normal series, solvable groups, composition series. Jordan-H lder theorem mentioned but not proved. Illustrated on examples. (not in the textbook)

6. Ring theory.
Definition of a ring, commutative ring, ring with unity. Zero divisors, invertible elements, domain, integral domain, division ring, field. Examples: Z, Z_n, Q, R, C, quaternions, square matrices with entries from the above, the power set with symmetric difference and intersection. Subrings. Necessary and sufficient condition for a subring. A subring of a domain is a domain. If 1 is the unity of a ring and belongs to a subring, then it is the unity of the subring. A division ring is a domain (homework). Example: 2Z_{10} \subset Z_10. (Chapter 4, Sections 1,2) Homomorphisms of rings. kernels of a homomorphism. Right ideal, left ideals and two-sided ideals. Factor rings. Homomorphism theorems and correspondence theorem for rings. Principal ideals, maximal ideals. (Chapter 4, Sections 3,4)

7. Polynomial rings.
Polynomials over commutative rings and over fields. Equality of polynomials. Division algorithm for polynomials over fields. Greatest common divisor of polynomials. Euclid algorithm. Relatively prime polynomial, irreducible polynomials, factorization. Principal ideals and maximal ideals of F[x]. Factorization. Euclidean rings. (Chapter