Math 4107 Study Sheet for the Final Exam

April 26, 2008

1. Know the basics of set theory, mappings, and properties of the integers, such as divisibility, gcds, the fundamental theorem of arithmetic, prime numbers, and congruences. Know how to prove that mappings are injective, surjective, and bijective. Know that f is invertible iff f is a bijection, as well as how to prove this. Know that compositions of surjections are surjections, compositions of injections are injections, and compositions of bijections are bijections. Know how to show that if $f : X \to Y$ is a bijection, then there is a bijection from $S_X \to S_Y$, where S_A denotes the set of bijections from $A \to A$.

2. Know the definition of a group, and how to prove that G is a group. Know some examples of groups, such as S_n, D_n, Z_n, and matrix groups. Know some examples of non-abelian groups, such as S_n, D_n and matrix groups. Know how to construct a group of order p^3 that is non-abelian, where p is a prime – basically, take 3×3 matrices in Z_p with 1's on the diagonal, 0's below the diagonal, and arbitrary Z_p elements above the diagonal.

3. Know the definition of a subgroup, and know how to quickly prove that $H < G$ is a subgroup of a group G. If G is finite you only need to check closure; that is, $h_1, h_2 \in H$ implies $h_1 h_2 \in H$. If G is not finite, you need to check that H contains the identity and that $h_1 \in H$, $h_2 \in H$ implies $h_1 h_2^{-1} \in H$. Know the "one step subgroup test": If $a, b \in H$ implies $ab^{-1} \in H$, and H is non-empty, and H is a subset of a group G, then H is a subgroup of G.

4. Know that if $H, K < G$, then $|HK| = |H||K|/|H \cap K|$, as well as the fact $HK < G$ if and only if $HK = KH$.

5. Know Lagrange's theorem, and know how to apply it to show that $|H|||G|$, as well as to prove Euler's theorem that if a is an integer coprime to n (meaning it has no common factors with n), then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Know how to prove that a relation is an equivalence relation. Know about cosets, and the index of a subgroup H in G, denoted by $[G : H]$.

6. Know normal subgroups. Know how to construct quotient groups.

7. Know homomorphisms and isomorphisms of groups, and how to prove that maps are homomorphisms and isomorphisms.

8. Know how to show and use the fact that normal subgroups can be realized as kernels of homomorphisms, and the fact that kernels are normal subgroups.

9. Know Cayley's theorem, which says that every group G can be embedded into a subgroup of a symmetric group. Recall that the symmetric group S on a set X, which I denote by S_X, is the set of all bijections $\varphi : X \to X$. The proof of Cayley's theorem amounts to taking X as the elements of the group, and then bijections $\varphi : X \to X$ that these elements correspond to is just left-multiplication. That is, if $g \in G$, and $X = G$, then associated to g we have a bijection $\varphi : X \to X$, where $\varphi(x) = gx$.

10. Be able to explicitly represent groups in terms of permuations. For instance, D_3 is isomorphic to S_3, where we can think of the rotation R by $2\pi/3$ radians as the cycle (1 2 3), and can think of a flip F as (1 2).

11. Cayley's theorem is intimately connected with actions. Know how to use Cayley's theorem and actions to prove that certain subgroups of a group G must be normal. One example of this is as follows: Suppose that G is a group of order $3p$, where $p \equiv 1 \pmod 3$ is prime. Let H be a subgroup of G of order p. Prove that H is normal (without invoking Sylow's theorem). If we let H act on the left-cosets of H by left-multiplication, since there are 3 cosets, this means that we get a mapping from $\varphi : H \to S_3$. Since H has order p, while S_3 has order 6, the kernel must be all of H. That is, H acts trivially on the left-cosets of H; that is, for every $h \in H$, and $a \in G$, $haH = aH$. This clearly implies $aH = Ha$, and therefore H is normal. You can reach similar sorts of conclusions by just letting G act on the cosets of H.

12. Know how to decompose a permutation into a product of disjoint cycles.

13. Know how to tell if a permutation is even or odd.

14. Know the relationship between the sign of a permutation, and the determinant of permutation matrices (this is not in your book – I only covered it in the lectures).

15. Know and be able to prove that the conjugates of a given permutation α are all those permutations with the same cycle structure as α.

16. Know how to find all the subgroups of S_4.

17. Be able to show that A_n (the alternating group) is generated by the 3-cycles.

18. Know how to show that S_n is generated by transpositions.

19. Know what the class equation is for conjugation: It is a way of writing $|G|$ as a sum of all the equivalence classes of elements under conjugation.

20. Be able to use the class equation to show that p-groups always have a non-trivial center.

21. Be able to prove that groups of order p^2 are abelian.

22. Be able to show that groups of order divisible by p have an element of order p (without invoking Sylow).

23. Know how to prove Sylow I in the usual way (this is actually the second proof in your book, and is on page 94).

24. Know the statements of all the Sylow theorems.

25. Know how to use the Sylow theorems to prove that certain subgroups are normal. For example, in a group of order 15, the 5-Sylow subgroup is normal, because the number of 5-Sylows is $1 \pmod 5$, and must divide 15, giving that there is only one; and then, since all Sylow-p subgroups are conjuagate, the Sylow-5 must be normal.

26. Be able to use the existence of Sylow-p subgroups to prove that groups are abelian. See, for example, the usual proof that all groups of order 15 are abelian, and cyclic.

27. Know the definition of internal direct product. Know the isomorphism between cartesian project and internal direct product. Know the group theory manifestation of the "Chinese Remainder Theorem" that I mentioned in class.

28. Be able to combine Sylow's theorem with various counting arguments to deduce that certain groups are not simple (simple means they have no non-trivial normal subgroups; so, non-simple means they have a normal subgroup). For example, in a group of order 30 you know that there are 1 or 10 Sylow-3 subgroups, and 1 or 6 Sylow-5 subgroups. You can show that either a Sylow-3 or a SYlow-5 is normal using a further counting argument as follows: If there were 10 sylow-3 subgroups, and 6 sylow-5 subgroups, then you would have 20 elements of order 3, and 24 elemetns of order 5, giving that G has at least $20 + 24 = 44$ elements, impossible.

29. Be able to combine normal Sylow subgroups with homomorphisms. For example, if a sylow subgroup P is normal in G, then you have a homomorphism $\varphi : G \to G/P$, which you can use to make further deductions.

30. Know the statement of the Fundamental Theorem of Finite Abelian Groups.

31. Know how to determine all non-isomorphic abelian groups of a given order.

32. Know how to count the number of non-isomorphic abelian groups of a given order (it is related to the partition function).

33. Know how to prove that certain abelian groups are non-isomorphic. For example, $Z_3 \times Z_3$ is not isomorphic to Z_9.

34. Know a few examples of non-abelian groups; for example, D_n, S_n, and matrix groups.

35. Know the definition of a ring, and know and be able to prove that certain sets with operations $+$ and $\cdot$ form a group. Examples abound: the integers, the real numbers, rationals, polynomials with integer rational complex coefficients, quaternions.

Here is an easier definition of a ring than the book: R is a ring if it is an abelian group under addion, and if it saties the usual multiplication relations $a, b, c \in R$ implies $ab \in R$, $a(bc) = (ab)c$, there exists $1 \in R$ such that $1a = a1 = a$, and finally we have the distributive rules, which are the only rules that connect the two operations $\cdot$ and $+$. These last rules are $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$. If R is commutative under $\cdot$, it is called a commutative ring.

36. Know basic properties of division rings, integral domains, fields. Know that finite integral domains are fields. Know the definition of characteristic and that integral domains always have either prime characteristic or 0 characteristic. Know the cancellation law for integral domains. Know that every integral domain contains either a copy of Z/pZ or the rationals Q. Know that Z/pZ is a field. Know the field of fractions construction. Know the definition of ring homomorphisms, ideals, quotient rings. Know that M is a maximal ideal of a ring R iff R/M is a field.

37. Know the definition of a field, an integral domain, a Euclidean domain, a principal ideal domain (so, know what principal ideals are), and a unique factorization domain.

38. Know the definition of ring homomorphisms and isomorphisms, and know how to show that kernels are ideals, and that an ideal of a ring can be realized as a kernel of some homomorphism. Know the first isomorphism for rings.

39. Know the book's definition of prime elements, irreducible elements of polynomial rings. Know how to show that if p is a prime element of a

PID, and $p|ab$, then $p|a$ or $p|b$ (on the exam, I will tell you which version of the definition of "prime element" to use). Know how to compute gcd's in Euclidean Domains, in particular in $Z[i]$, and know how to use the d function $d(x+iy) = x^2 + y^2$ to prove various things.

40. Know the fact that fields have only trivial ideals. Know that if f is a non-trivial homomorphism out of a field, then f must be injective. Know the fact that if D is a domain, and I is a maximal ideals of D, then D/I is a field. Know the characteristic of a domain. Know the fact that every finite integral domain is a field.

41. Understand the proof that if D is a Euclidean Domain, then D is also a UFD; also, know the fact that this holds more generally for PID. In particular, know how to show $F[x]$ is a ED, where F is a field; so, $F[x]$ is a UFD. Know the obvious example showing the $Z[x]$ is not a PID (The example is I is the set of all polynomials with an even constant coefficient. Another way to describe I is that it is the set of all polynomials $f(x)$ where $f(0)$ is even.)

42. Know basic properties about the content of a polynomial, and understand how to use it to show that $Z[x]$ is a UFD. Know Gauss's Lemma and Eisenstein's criteria for irreducibility.

43. Know the fact that if F is a field, then $F[x]$ is a UFD. Know that if R is a UFD, then so is $R[x]$, and in fact, $R[x_1, ..., x_k]$.