SF2714 Discrete Mathematics and Algebra, Fall 2009
Jakob Jonsson

**Important concepts**

To make sure nobody spends time memorizing unnecessary concepts and formulas, here is an overview of what is important in this course. As a general principle, do not try to remember long and technical proofs in Biggs or the Lecture Notes.

On the final exam, you will be given the definitions of the following concepts: chromatic polynomial of a graph, isomorphism of graphs, homomorphism or isomorphism of groups, automorphism group of a graph, left and right coset of a group, orbit of a group on a set, stabilizer, ring or field of congruence classes modulo a polynomial.

LN = Lecture Notes.

**Lecture 1.** Equivalence relations and classes play a central role in this course. Make sure you fully understand these concepts.

**Lecture 2.** The concepts in this lecture are very important, especially the main results, i.e., Theorems 2.1-5 in LN. For given integers $a$ and $b$, you should know how to find integers $m$ and $n$ such that $am + bn = \gcd(a, b)$. Instead of memorizing formula (1) in LN, try to understand why the formula looks the way it does.

**Lecture 3.** The "principles of counting" are just formalizations of concepts that you are most likely already familiar with. The most important fact about Euler's function is its definition and Theorem 3.6 in LN. Theorems 3.8-9 are not important in this course. The Chinese Remainder Theorem appears in a later lecture and may be skipped at this point. The connection between functions, words and permutations is important.

**Lecture 4.** The binomial numbers and binomial theorem are very important. Regarding the formula for the number of unordered selections, you should focus on understanding the basic ideas behind the proof, not the formula itself. The same goes for the sieve principle. Do not bother with all technical details of the proof of Theorem 4.7 in LN. Instead, look at some special cases (say $k = 2, 3, 4$), and try to reconstruct the formula for these cases.

**Lecture 5.** Partitions of sets are very important objects, so make sure you understand how they work. You do not need to remember the definitions of Stirling numbers, Bell numbers and multinomial numbers, but you should understand the proof of Theorem 12.3.2 in Biggs. Permutations are also very important,

and you should be familiar with the cycle representation. The proof of Theorem 12.5 in Biggs is more important than the theorem itself. Don't memorize the proof, but make sure you understand the underlying principle.

**Lecture 6.** Congruences are very important. Make sure you understand everything in Sections 6.1-2 in LN. Section 6.3 contains results that are special cases of group-theoretic results proved later in the course. There will be no exam problems requiring that you remember Theorem 6.9 in LN (but you should feel free to use this theorem if you indeed find a way to apply it).

**Lecture 7.** You should be acquainted with the concepts of isomorphic graphs, cycles, connected components, Hamiltonian cycles and trees. You do not have to remember the exact formulation of the theorems. When looking at the proofs, try to understand the main ideas, not the technical details.

**Lecture 8.** You can skim through the section about the chromatic number and concentrate on the chromatic polynomial. You will gain from knowing the deletion-contraction principle in Theorem 8.7 and the simple rules given in Propositions 8.5-6. Skim through the section about bipartite graphs and matchings.

**Lecture 9.** We introduced several extremely important concepts in this lecture: the four axioms of a group, the property of being abelian and the order of a group element. Isomorphisms of groups are also important. Make sure you understand what it means to prove the identity $\varphi(ab) = \varphi(a)\varphi(b)$.

**Lecture 10.** Again, there are several important concepts introduced: cyclic groups, direct products of groups, subgroups, cosets and Lagrange's Theorem. Everything in Section 10.4 in LN is important. Theorem 10.2 and Propositions 10.4-5 are just illustrating examples to help you understand the various concepts.

**Lecture 11.** Regarding the characterization of the cyclic group $C_n$ in Theorem 11.1 in LN, what is really important is that $C_n$ has the stated properties. The remark after the proof of the theorem is also important. Section 11.2 in LN can be read as an introduction to section 11.3. Regarding the latter section, I will remind you of the definitions of orbits and stabilizers. Instead of trying to remember Theorem 11.4, focus on Lagrange's Theorem (Theorem 10.9) and Theorem 12.1, which are more important in applications.

**Lecture 12.** You should be able to apply Theorem 12.1 in LN to simple examples such as cyclic groups and the group of symmetries of a square. You do not need to remember the formula in Proposition 12.2. In the section about rings, you should understand the definition and know that $\mathbb{Z}$, $\mathbb{Z}_m$ and $R[x]$ (introduced later) are rings. We will only consider commutative rings. Fields are very important throughout the remainder of the course.

**Lecture 13.** Make sure you notice the analogous properties of polynomials and integers (the division algorithm and so on). Just as for integers, the Euclidean algorithm is very important. You should also know that factorization of polynomials over fields is unique and remember the results mentioned in Section 13.4 in LN. The technique described on page 312 in Biggs (and also in Section 14.2 in LN) is very important.

**Lecture 14.** Again, note the analogous properties of congruences modulo polynomials and integers. You must know that $F[x]/k(x)$ is a field if and only if $k(x)$ is irreducible. Look carefully at the examples in Section 14.2. You must also know that the order of a field is a prime power and that the characteristic of a finite field is a prime. You may skim through the proof of Theorem 14.4.

**Lecture 15.** The concept of primitive elements is very important. You should know that the multiplicative group of a field is cyclic. When looking for primitive elements, you might find Propositions 15.2-3 helpful, but it might be sufficient to remember that the order of an element divides the order of the group. Regarding codes, you should know the basics of the Hamming distance and the important Theorem 15.4 in LN. In Theorem 15.5, you may concentrate on $e = 1$.

**Lecture 16.** You should know that a linear code is a subgroup of $(\mathbb{Z}_2)^n$ and also know the definition of a check matrix. Theorems 16.1 and 16.3 are important, and you should also know how to correct errors in a Hamming code. Yet, you may skim through Proposition 16.2 (this is stuff not mentioned at all in Biggs).