**MAT 312/AMS 351 Spring 2012 Review for Midterm 2**

§1.6 Understand the principle of factorization-based public-key codes, as explained in the Example on p.72. Try Exercises 12, 13 on pp.76,77.

§4.1 Remember that in the product permutation $\pi\sigma$ the $\sigma$ permutation is performed first. Know simple examples, say with $n = 3$, where $\pi\sigma \neq \sigma\pi$. Be able to read off the inverse of a permutation from its "two-row" representation, p.152 (Exercise 2 p.158). Know the definition of a cycle (p.152) and be able to represent any permutation (given, for example, in "two-row" notation) as a product of disjoint cycles. Be comfortable myltiplying cycles (p.156). Exercise 4 p.158.

§4.2 Understand that powers of a single permutation multiply following the law of exponents (Theorem 4.2.1), and that $(\pi\sigma)^r = \pi^r\sigma^r$ if $\pi\sigma = \sigma\pi$ and not, in general, otherwise. Understand why every permutation $\pi$ of the $n$ objects $1, 2, \ldots, n$, i.e. $\pi \in S(n)$, has some power equal to the identity (Theorem 4.2.2), and the definition of the *order* of a permutation, p.161. Understand that if $\pi$ is a cycle of length $k$, then the order of $\pi$ is exactly $k$ (Theorem 4.2.4). Understand why, if $\pi$ is the product of *disjoint* cycles $\pi = \tau_1 \cdot \cdots \cdot \tau_p$, then $o(\pi) = \text{l.c.m.}(o(\tau_1), \ldots, o(\tau_p))$. Exercises 6, 7, 10 p.168.

Understand that the *sign* $\text{sgn}\pi$ of a permutation $\pi \in S(n)$ can be defined as $+1$ or $-1$ so that if $\sigma, \pi \in S(n)$ then $\text{sgn}(\sigma\pi) = \text{sgn}\sigma \cdot \text{sgn}\pi$ and the sign of any transposition is $-1$. Understand how every cycle of length $k$ can be written as a product of $k-1$ transpositions (Theorem 4.2.10), and consequently has sign $(-1)^{k-1}$. Understand how this calculation can be extended to any permutation (Theorem 4.2.11).

§4.3 Understand that the set $S(n)$ with the operation $(\sigma, \pi) \to \sigma\pi$ satisfies conditions (G1), ..., (G4) (p.170) and is therefore a *group*. [(G1) is often incorporated into the definition of the operation as a function from $G \times G$ to $G$.] Be comfortable with the notation $e$ or 1 for the unit element when the group is described multiplicatively, and 0 when the group is described additively (only done if the group is commutative). Know how to prove Theorem 4.3.1 (uniqueness of identity and of inverses). Be familiar with Examples 2 ($\mathbf{Z}_n$, addition) and 3 ($G_n$, the invertible elements of $\mathbf{Z}_n$, multiplication). Understand that the set of permutations in $S(n)$ which have even order is a subgroup (the "alternating group" $A(n)$) of $S(n)$. Understand that the set of $2 \times 2$ matrices with non-zero determinant form a group under matrix multiplication. [Here you need to check (G1); it is satisfied because the determinant $\det(AB)$ of the product of two matrices is the product $\det A \det B$ of their determinants]. Examples 2 and 3 give subgroups. Exercises 2, 3, 8.

§5.1 Understand that the "arithmetic" of elements in a group is completely similar to what we are used to from multiplication of non-zero real [or rational] numbers *except* that elements don't commute, in general. This is how to understand Theorem 5.1.1 and Examples 1, 2, 3, p.203. Furthermore the definition

and calculus of powers and order are exactly what we did for permutations. Subgroups are defined explicitly on p.206 (we already have some examples from permutations and from matrices; see Examples 3, 4, 5 p.208). Note part (iii) of Theorem 5.1.5 gives a 1-line characterization of a subgroup. Understand the definition of *proper* subgroup. Be able to prove Theorem 5.1.6 (intersection of 2 subgroups is a subgroup) and Theorem 5.1.7 (set of (positive and negative) powers of an element $g$ is a subgroup; called the "cyclic" subgroup generated by $g$, and denoted $\langle g \rangle$. Understand Examples 1, 2, 3, 4 pp.209-210. Review homework exercises.

§5.2 Understand the definition of *left coset* $aH$ and *right coset* $Ha$ corresponding to a subgroup $H$ of a group $G$ and an element $a \in G$. Understand the Notes on pp.212-213, and the 4 Examples given pp.213-214. Be able to repeat the analysis of Example 3 for different $G$ and $H$, e.g. $G = S(4), H = \langle (1234) \rangle$, etc. Be able to prove Theorem 5.2.1 (different cosets do not overlap). Understand how this implies Theorem 5.2.2: If the order of $G$ is finite, any two cosets of a subgroup $H$ have the same number of elements. And how this in turn implies Theorem 5.2.3 (Lagrange's Theorem): the order of $H$ must divide the order of $G$. (The quotient is called the *index* of $H$ and written $[G : H]$). Understand this special case: the order of the element $g \in G$ is the order of the subgroup $\langle g \rangle$ and therefore must divide the order of $G$. Exercises 1, 2, 5 pp.218-219.

§5.3 Besides the definitions in the book, understand that for groups $G_1, *$ and $G_2, \circ$ a function $\theta : G_1 \to G_2$ is a *homomorphism* if it respects the group operations: $\theta(g * g') = \theta(g) \circ \theta(g')$. A homomorphism which is a bijection (one-one and onto) is an *isomorphism*. Example 3 p.221 is a homomorphism but not an isomorphism. Be able to prove Theorem 5.3.1 for homomorphisms as well as for isomorphisms. Be able to explain why $G_5$ and $G_8$ are not isomorphic, even though they are both abelian (commutative) with four elements. Understand the definition of the *direct product* $G \times H$ of groups $G$ and $H$. Be able to construct an isomorphism $G_8 \to C_2 \times C_2$ (we use $C_n$ for the cyclic group of order $n$, written multiplicatively). Be able to prove that if $(m, n) = 1$ then $C_m \times C_n$ is cyclic; or, in additive notation, $\mathbf{Z}_m \times \mathbf{Z}_n$ is cyclic. Be able to prove that every group of prime order is cyclic. Understand the argument p.226 that if $G$ is a group of of order 6 with no element of order 6 then it must have an element of order 3.