Math 412. Final Exam review questions

Groups

- Definition of groups
  - What is a group?
  - How many identity elements are there in a group?
  - How may inverses are in a group?
  - When does $gx = h$ have a solution in a group? How many solutions?
  - What is a subgroup of a group?
  - What two "trivial" subgroups does every group have?
  - Is the empty set a subgroup?
  - What is an abelian group?
  - What is the order of a group?
  - What is the order of an element of a group?
  - What is the order of a subgroup?
- Examples of groups
  - If R is a ring, R with which operation is a group?
  - If R is a ring, what subset of R is a group under $\times$?
  - What is the group $\mathcal{S}_n$? What is its order?
  - What is the group $\mathcal{A}_n$? What is its order?
  - If X is a set, why is $\mathrm{Bij}(X)$, the set of bijections of X, a group?
  - What is the group D_n? What is its order?
  - What is the group of rotational symmetries of a cube? What is its order?
  - If $\mathbb{F}$ is a field, what is $\mathrm{GL}_n(\mathbb{F})$? What is the order of $\mathrm{GL}_2(\mathbb{F})$?
  - What is the group $\mathrm{SL}_n(\mathbb{F})$?
  - What is the group $\mathbb{Z}_n^\times$?
  - Is $D_n \cong S_n$?
  - Is $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$?
- Cyclic groups and generators
  - What is a cyclic group?
  - How many cyclic groups are there of order n, up to isomorphism?
  - What is the cyclic subgroup $\langle g \rangle$ generated by an element g in G?
  - What is the order of $\langle g \rangle$?
  - What are the orders of elements in a cyclic group of order n?
  - What are the subgroups of a cyclic group of order n?
  - What is the subgroup $\langle g_1, \dots, g_t \rangle$ generated by elements $g_1, \dots, g_t \in G$?
  - How many elements are needed to generate $\mathbb{Z}_n$?
  - How many elements are needed to generate D_n?
  - How many elements are needed to generate $\mathcal{S}_n$?
  - How many elements are needed to generate $\mathbb{Z}_p^\times$?
- Homomorphisms
  - What is a group homomorphism?
  - What is the kernel of the group homomorphism?
  - What special type of subset is the kernel of a homomorphism?
  - What special type of subset is the image of a homomorphism?
  - If ϕ is a homomorphism, what is $\phi(e_G)$?
  - If ϕ is a homomorphism, what is $\phi(g^{-1})$?
  - What is an isomorphism?

  - What does it mean for two groups G,H to be isomorphic?
  - If G and H are isomorphic, what can you say about their orders?
  - If G and H are isomorphic, what can you say about the orders of their elements?
  - Why is $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$ when p and q are distinct primes?
  - Why is $\mathbb{Z}_{pq}^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$ when p and q are distinct primes?
- Group actions
  - What is a group action?
  - What is the orbit of an element in a set X with an action of a group G on X?
  - What is the stabilizer of an element in a set X with an action of a group G on X?
  - How are the size of an orbit and the size of a stabilizer related?
  - How does the size of an orbit in a group action on X compare to the size of X?
  - How does the size of an orbit in a group action of G on X compare to the order of G?
  - How do orbits of the group action relate to each other?
  - When is a group action faithful?
  - If G acts on X, then there is an associated homomorphism from G to what group?
  - What are two examples of sets that $\mathcal{S}_n$ acts on?
  - What are two examples of sets that D_n acts on?
- The symmetric group
  - What is a permutation?
  - What is a t-cycle?
  - What are disjoint cycles?
  - What is permutation stack notation?
  - How do you convert an element from stack notation to disjoint cycle notation?
  - How do you rewrite a product of cycles as a product of disjoint cycles?
  - How do you find the order of an element in $\mathcal{S}_n$?
  - What is an even permutation?
  - What is an odd permutation?
  - What is the sign homomorphism?
- Cosets and Lagrange's Theorem
  - What is a right coset of H in G?
  - What is a left coset of H in G?
  - What is the index of H in G?
  - State Lagrange's Theorem in terms of the order of a group, order of a subgroup, and index.
  - What is the relationship between the order of a subgroup and the order of the group?
  - What is the relationship between the order of an element and the order of the group?
  - What is $[a^{p-1}]_p$ if p is prime?
  - What is $[a^n]_{pq}$ if p, q are prime and $n \equiv 1 \bmod (p-1)(q-1)$?
- Normal subgroups
  - What is a normal subgroup, in terms of left and right cosets?
  - What is a normal subgroup, in terms of gNg^{-1}?
  - When is a subgroup normal, in terms of conjugacy classes?
  - Associated to every homomorphism is what normal subgroup?
  - What is an example of a normal subgroup of D_n?
  - What is an example of a normal subgroup of $\mathcal{S}_n$?
  - A normal subgroup is always the kernel of which group homomorphism?

- Quotient groups
  - When does a subgroup define a quotient group?
  - What are the elements of a quotient group?
  - How do you tell if two elements of a quotient group are the same?
  - What is the operation on a quotient group?
  - Why is the property that N is normal important to define a quotient group?
  - How is the order of a quotient group related to the order of the group?
  - What is a homomorphism from G to G/N?
  - What are the quotient groups of a simple group?
  - Is a quotient of a cyclic group cyclic?
  - Is a quotient of an abelian group abelian?
  - Is a quotient of an infinite group infinite?
  - What does the first isomorphism theorem say?
  - Given a homomorphism, what quotient of the source is isomorphic to the image?
  - How does the cardinality of the image of a homomorphism relate to the order of the source?
- Simple groups
  - What is a simple group?
  - What abelian groups are simple?
  - For what values of n is there an abelian simple group of order n?
  - Is every simple group abelian?

RINGS

- Definition of ring
  - What is an operation?
  - What does it mean to be associative?
  - What does it mean to be commutative?
  - What does it mean to have an identity?
  - What does it mean for an element to have an inverse?
  - What does it mean for two operations to satisfy distributive laws?
  - What is the definition of a ring?[1]
  - What is the definition of a subring?
  - How do you define subtraction in a ring?
  - Can you use the axioms to prove that $(-a)(-b) = ab$, and other basic things?
- Examples/constructions of rings
  - Which familiar sets of numbers are rings?
  - Is $\mathbb{Z}_N$ a ring? What are the operations?
  - Why is $R \times S$ a ring if R, S are? What the the operations, and 0 and 1?
  - How do you check if a subset of a ring is a subring?
  - Do you know rings where the multiplication is not commutative?
  - Are there infinite rings with finite subrings?
  - Are there commutative rings with noncommutative subrings?
  - Are there noncommutative rings with commutative subrings?
- Special types of rings/elements
  - When does $0 = 1$ in a ring?
  - What is a commutative ring?
  - What is an (integral) domain?

[1] A ring always has a multiplicative identity in this class.

- What is a field?
- Which of the last few notions imply each other? Why? What if the ring is finite?
- Can you cancel addition in a ring?
- Can you cancel multiplication by a nonzero element in a ring? If not, can you do it in one of the special types of rings above?
- What is a zerodivisor? What does it have to do with these special ring types?
- What is a unit? What does it have to do with these special ring types?
- What is a nilpotent?
- What is an idempotent?
- In what type of ring do you have all four operations $+, -, \times, \div$ (except dividing by zero)? How is division defined in such a ring?

- Homomorphisms
  - What is a homomorphism?
  - What is an isomorphism?
  - Can you find homomorphisms that are injective but not surjective? Surjective but not injective? Neither?
  - What is the kernel of a homomorphism?
  - What is the image of a homomorphism?
  - What special property does the kernel have?
  - What special property does the image have?
  - When is there a homomorphism $\mathbb{Z}_N \to \mathbb{Z}_M$?
  - Given a ring R, what ring homomorphisms $\mathbb{Z} \longrightarrow R$ are there?
- Ideals
  - What is an ideal?
  - How do you check a subset of a ring is an ideal?
  - Are ideals subrings? Are subrings ideals?
  - What two ideals does every ring have?
  - How is checking a subset is an ideal different in a commutative ring vs a noncommutative one?
  - What is the ideal generated by $a_1, \ldots, a_t$ in a commutative ring?
  - What are generators of an ideal?
  - What is congruence modulo an ideal?
  - Must every ideal I in a ring R be the kernel of some ring homomorphism $R \longrightarrow S$?
- $\mathbb{Z}$
  - What is the division algorithm in $\mathbb{Z}$?
  - What is the Euclidean algorithm in $\mathbb{Z}$?
  - What is the fundamental theorem of arithmetic in $\mathbb{Z}$?
  - What are the units in $\mathbb{Z}$?
  - What are the zerodivisors in $\mathbb{Z}$?
  - What is the GCD of two elements in $\mathbb{Z}$?
  - What is a prime in $\mathbb{Z}$?
  - What special property do primes have for dividing other numbers?
  - Is the GCD of two integers a linear combination? How do you find it as such?
  - What are the ideals in $\mathbb{Z}$?
  - What rings can we obtain as quotients of $\mathbb{Z}$?
- $\mathbb{Z}_N$
  - What is $\mathbb{Z}_N$? What are its elements?
  - What are the units in $\mathbb{Z}_N$?
  - What are the zerodivisors in $\mathbb{Z}_N$?

  - When is $\mathbb{Z}_N$ a field? A domain?
  - For which N does $ax = b$ always have a solution in $\mathbb{Z}_N$, if $a \neq 0$?
  - How do you find inverses in $\mathbb{Z}_N$?
  - How do you solve $ax = b$ in $\mathbb{Z}_N$, when it does have a solution?
  - What are the ideals in $\mathbb{Z}_N$?
  - What does the Chinese remainder theorem say?
- $\mathbb{F}[x]$
  - What is the division algorithm in $\mathbb{F}[x]$?
  - What is the fundamental theorem of arithmetic in $\mathbb{F}[x]$?
  - What are the units in $\mathbb{F}[x]$?
  - What are the zerodivisors in $\mathbb{F}[x]$?
  - What is the GCD of two elements in $\mathbb{F}[x]$?
  - What is an irreducible element in $\mathbb{F}[x]$?
  - What special property do irreducible element for dividing other numbers?
  - Is the GCD of two polynomials in $\mathbb{F}[x]$ a linear combination? How do you find it as such?
  - What are the ideals in $\mathbb{F}[x]$?
  - What is the relationship between roots of $f(x) \in \mathbb{F}[x]$ and linear factors of $f(x)$?
  - Why does a polynomial of degree ≤ 3 with no roots in $\mathbb{F}[x]$ have to be irreducible?
  - Does every polynomial in $\mathbb{F}[x]$ with no roots have to be irreducible?
- $R[x]$ for a general ring R
  - When is $R[x]$ a domain, if R is commutative?
  - If R is a domain, what are the units in $R[x]$?
  - Is every ideal of $R[x]$ generated by one element, in general?
  - Is there a division algorithm for $R[x]$ in general?
  - How is $\deg(fg)$ related to $\deg(f)$ and $\deg(g)$?
  - What if R is a domain?
- Quotient rings
  - What is a quotient ring?
  - What are the elements in R/I?
  - What are the operations in R/I?
  - What does the first isomorphism theorem say?
- $\mathbb{F}[x]/(f)$, for $\mathbb{F}$ a field and $f \in \mathbb{F}[x]$
  - What is $\mathbb{F}[x]/(f)$? What are its elements?
  - What are the units in $\mathbb{F}[x]/(f)$?
  - What are the zerodivisors in $\mathbb{F}[x]/(f)$?
  - When is $\mathbb{F}[x]/(f)$ a field? A domain?
  - For which f does $ax = b$ always have a solution in $\mathbb{F}[x]/(f)$, if $a \neq 0$?
  - How do you find inverses in $\mathbb{F}[x]/(f)$?
  - How do you solve $ax = b$ in $\mathbb{F}[x]/(f)$, when it does have a solution?
  - What are the ideals in $\mathbb{F}[x]/(f)$?