Math 393: The Final Exam Study Sheet.

1. Know the basic definitions (groups, order, normal subgroups, rings, subrings, integral domains, division rings, fields, ideals (including prime and maximal), units, group/ring homomorphisms and isomorphisms, cosets, quotient group/rings). Also know how to test for a set to be a subgroup/subring.

2. Examples of groups and rings:
   (a) Cyclic groups (finite: \( \mathbb{Z}_n \) and \( \mathbb{U}_n \), and infinite: \( \mathbb{Z} \)) and their basic properties (structure of subgroups, locating generators, etc.)
   (b) Nonabelian groups (especially \( D_n \), \( S_n \), and \( A_n \))
   (c) Misc. groups (\( V_4 \), \( Q_8 \), matrix groups, \( Q \), \( \mathbb{R}, \mathbb{C} \), direct products and quotients)
   (d) Rings (\( \mathbb{Z}, \mathbb{Z}_n, \mathbb{R}[x], M_m \times n(R) \), direct products and quotients, etc.)
   (e) Integral Domains (\( \mathbb{Z}, \mathbb{Z}_p \), \( \mathbb{R}[x] \) when \( R \) is an integral domain)
   (f) Division Rings/Fields (Noncommutative: \( \mathbb{H} \), Fields: \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p \), and \( \mathbb{F}_{p^k} \))

3. Know these proofs:
   - Fermat’s Little Theorem/Euler’s Theorem (via Lagrange’s Theorem).
   - The kernel of a group homomorphism \( f : G \to G' \) is a normal subgroup of \( G \).
   - Finite integral domains are fields.
   - An ideal \( P \) of a ring \( R \) is prime iff \( R/P \) is an integral domain.
   - Chinese Remainder Theorem (\( \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \) when \( \gcd(m, n) = 1 \)).

4. Sample questions:
   (a) Show that \( \mathbb{R} \) (with addition) is not isomorphic to \( \mathbb{R}^* \) (with multiplication).
   (b) To which familiar group is \( \mathbb{Q}_8 = \{ \pm 1 \} \) isomorphic? Explain.
   (c) Define \( (\mathbb{Q}^*)^2 = \{ q^2 : q \in \mathbb{Q}^* \} \). Describe the quotient group \( \mathbb{Q}^*/(\mathbb{Q}^*)^2 \).
   (d) Find a generator for \( \mathbb{Z}_{11}^* \). What are the other generators. Use one of the generators to explicitly display an isomorphism between \( \mathbb{Z}_{10} \) and \( \mathbb{Z}_{11}^* \).
   (e) Let \( I \) be an ideal of a noncommutative ring \( R \) such that \( ab - ba \in I \) for all \( a, b \in R \). Show that \( R/I \) is commutative.
   (f) Suppose that \( C \) and \( D \) are ideals of \( A \) and \( B \), respectively. Show that \( C \times D \) is an ideal of \( A \times B \), and \( (A \times B)/(C \times D) \cong A/C \times B/D \), by examining the ring homomorphism \( f : A \times B \to A/C \times B/D \) defined by \( f(a, b) = (a + C, b + D) \).
   (g) Describe how to construct a field with 16 elements. Be able to add, multiply, and invert elements in this field. How many such fields are there up to isomorphism?
   (h) Show that \( \langle 2, x \rangle \) is not a principal ideal of \( \mathbb{Z}[x] \) (i.e., generated by one polynomial in \( \mathbb{Z}[x] \)). Is this ideal prime and/or maximal? Explain.
   (i) Show that there does not exist an integral domain with 6 elements.
1. Let $R$ be a finite integral domain. Then, $R$ is a field.

**Proof:** We need to show that any nonzero $a \in R$ has a multiplicative inverse in $R$. To this end, fix $a \in R$, and consider the map $L : R \to R$ defined by $L(r) = ar$. $L$ is 1-1, because if $L(r) = L(s)$ for some $r, s \in R$, then $ar = as$, or equivalently $ar - as = a(r - s) = 0$. Since $R$ is an integral domain and $a \neq 0$, we have $r - s = 0$, and hence $r = s$. Since $L$ is 1-1 from $R$ to itself, and $R$ is finite, we conclude that $L$ is also onto (and thus we have a bijection). In particular, there exists $r \in R$ such that $L(r) = ar = 1$. ■

2. Show that $\mathbb{R}$ (with addition) is not isomorphic to $\mathbb{R}^*$ (with multiplication).

**Proof:** Suppose $f : \mathbb{R} \to \mathbb{R}^*$ is an isomorphism. Then, we know have for any $x \in \mathbb{R}$ that $f(x) = f(x/2 + x/2) = [f(x)]^2 \geq 0$. This contradicts $f$ being onto. Alternately, $\mathbb{R}^*$ has an element of order 2 (namely $-1$), while $\mathbb{R}$ has no element of order 2. ■

3. To which familiar group is $Q_8/\{\pm 1\}$ isomorphic?

**Solution:** Let $N = \{\pm 1\}$. So, $Q_8/N = \{N, iN, jN, kN\}$, all of which have orders no more than 2. Hence, This is isomorphic to $V_4$, the Klein 4-Group. ■

4. Define $(\mathbb{Q}^*)^2 = \{q^2 : q \in \mathbb{Q}^*\}$. Describe the quotient group $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

**Solution:** $\mathbb{Q}^*/N = \{mN : m \text{ is a squarefree integer}\}$. ■

5. Find a generator for $\mathbb{Z}_{11}^*$. What are the other generators. Use one of the generators to explicitly display an isomorphism between $\mathbb{Z}_{10}$ and $\mathbb{Z}_{11}^*$.

**Solution:** One such generator for $\mathbb{Z}_{11}^*$ is 2. So, an isomorphism $f : \mathbb{Z}_{10} \to \mathbb{Z}_{11}^*$ can be defined by sending one generator to another, such as $f(1) = 2$, or more explicitly $f(n) = 2^n$. ■

6. Let $I$ be an ideal of a noncommutative ring $R$ such that $ab - ba \in I$ for all $a, b \in R$. Show that $R/I$ is commutative.

**Proof:** Let $x + I, y + I \in R/I$ for some $x, y \in R$. Then, $xy + I = xy + (yx - yx) + I = yx + I$, showing that $R/I$ is commutative. ■

7. Suppose that $C$ and $D$ are ideals of $A$ and $B$, respectively. Show that $C \times D$ is an ideal of $A \times B$, and $(A \times B)/(C \times D) \cong A/C \times B/D$, by examining the ring homomorphism $f : A \times B \to A/C \times B/D$ defined by $f(a, b) = (a + C, b + D)$.

**Proof:** Check that this is a ring homomorphism which is onto (straightforward). Next, $\ker f = \{(a, b) \in A \times B : f(a, b) = (a + C, b + D) = (0 + C, 0 + D)\} = \{(a, b) : a \in C, b \in D\} = C \times D$. The result now follows from the First Isomorphism Theorem. ■
8. Describe how to construct a field with 16 elements. Be able to add, multiply, and invert elements in this field. How many such fields are there up to isomorphism?

**Solution:** Note that $16 = 2^4$. So, $\mathbb{F}_{16} \cong \mathbb{Z}_2/(p(x))$, where $f(x)$ is an irreducible polynomial over $\mathbb{Z}_2[x]$ of degree 4. One such $f$ is $f(x) = x^4 + x + 1$. ■

9. Show that $\langle 2, x \rangle$ is not a principal ideal of $\mathbb{Z}[x]$ (i.e., generated by one polynomial in $\mathbb{Z}[x]$). Is this ideal prime and/or maximal? Explain.

**Proof:** Suppose to the contrary that $\langle 2, x \rangle = \langle f(x) \rangle$ for some $f(x) \in \mathbb{Z}[x]$. So, we have $2 = g(x)f(x)$ and $x = h(x)f(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$. The first equation implies that $f(x)$ is constant, and in particular $f(x) = 1$ or $2$ (up to associates, which are irrelevant for generators). If $f(x) = 1$, then $\langle f(x) \rangle = \mathbb{Z}[x]$, which is a contradiction, because $\langle 2, x \rangle$ is a proper ideal of $\mathbb{Z}[x]$ (for instance, $1 \notin \mathbb{Z}[x]$).

Otherwise, $f(x) = 2$, and thus $x = 2h(x)$, which implies that $h(x) = x/2 \notin \mathbb{Z}[x]$, which again is a contradiction.

Since $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}_2$, which is both an integral domain and a field, we see that $\langle 2, x \rangle$ is both prime and maximal. ■

10. Show that there does not exist an integral domain with 6 elements.

**Proof:** Suppose to the contrary that there exists an integral domain $R$ with 6 elements. Since $R$ is a ring, it is an abelian group with respect to addition. So, $R \cong \mathbb{Z}_6$ as groups. Then, $\text{char}(R) = 6$, which contradicts the fact that an integral domain has zero or prime characteristic. ■