Dartmouth College Department of Mathematics
**Math 71 Algebra**
Fall 2023

Final Exam Review Sheet

**Directions:** The final exam will take place in Kemeny 105 (our usual classroom) on Monday, November 20 from 3:00–6:00 pm. No electronic devices will be allowed. No notes will be allowed. On all problems, you will need to write your thoughts/proofs in a coherent way to get full credit.

**Topics covered and practice problems:**

- Basic set theory and functions (injections, surjections, bijections). Definition of a group. Presentation with generators and relations. Modular arithmetic. Multiplicative group modulo $n$. DF 0.1 Exercises 4–6; DF 0.2 Exercises 7, 8, 11; DF 0.3 Exercises 4, 5, 7, 9; DF 1.1 Exercises 1, 2, 5–9, 12–14, 21, 28, 31, 36.
- Dihedral groups. Symmetric groups. Disjoint cycle decomposition of permutations. Matrix groups over a field. Alternating groups. DF 1.2 Exercises 4–6, 9; DF 1.3 Exercises 9–19; DF 1.4 Exercises 7, 10; DF 3.5 Exercises 1–4, 6, 8, 9, 12,
- Homomorphisms and isomorphisms. Kernel. Image. DF 1.6 Exercises 3–9, 11, 15–16, 19, 21–22, 25.
- Group actions. Permutation representation. Kernel. Faithful. Transitive. Orbit. Stabilizer. Left multiplication action. Conjugation action. Conjugacy classes. Cycle type and conjugacy in the symmetric group. Orbit-stabilizer theorem. Class equation. $A_5$ is simple. $p$-groups have nontrivial center. Groups of order $p^2$ are abelian. DF 1.7 Exercises 1–3, 5–6, 8–13, 20, 21, 23; DF 4.1 Exercises 1–6; DF 4.2 Exercises 1–3; DF 4.3 Exercises 2–3, 7, 10–12, 6–12, 25, 28–29.
- Subgroups. Cyclic subgroups. Centralizers. Generators. Lattice of subgroups. DF 2.1 Exercises 1–5, 14; DF 2.2 Exercises 1, 3, 7–8, 14; DF 2.3 Exercises 1–5, 10–14, 25, 26; DF 2.4 Exercises 5–9, 11–14; DF 2.5 Exercises 3, 5, 7, 9–10, 12–13, 15.
- Quotient groups. Cosets. Isomorphism theorems. Composition series. Simple groups. Solvable groups. DF 3.1 Exercises 6–13, 33–35; DF 3.2 Exercises 8, 13–17, 21–23; DF 3.3 Exercises 1, 4, 10; DF 3.4 Exercises 1–2 (just do $D_8$).
- Sylow $p$-subgroups. Sylow's Theorem. Number of Sylow $p$-subgroups. Applications to groups of small order: $pq$, $pqr$, $2^k \cdot 3$, $4 \cdot 3^k$, 56, etc. DF 4.5 Exercises 4–9, 13–28, 39–40, 45, 56.
- Direct products. Fundamental theorem of finitely generated abelian groups. Invariant factors and elementary divisors. DF 5.1 Exercises 1, 4, 10, 14, 18; DF 5.2 Exercises 1–6, 9, 10, 15; DF 5.3 Just Read It.
- Rings. Division rings. Quaternion rings. Quadratic fields. Quadratic integer rings. Matrix rings. Polynomial rings. Group rings. Subrings. Zero divisors. Nilpotent elements. Group of units. Integral domains. Finite integral domain is a field. DF 7.1 Exercises 3–6, 8, 12, 13, 14, 17, 24, 25, 29; DF 7.2 Exercises 1–4, 5a, 6, 9–11.
- Ring homomorphisms. Ideals. Quotient rings. Isomorphism theorems for rings. Prime ideals. Maximal ideals. DF 7.3 Exercises 1–14, 18–21, 23, 24–26, 28, 31–32, 34, 36–37; DF 7.4 Exercises 4–9, 11, 13–19, 22, 27.
- Euclidean domains. Principal ideal domains. Unique factorization domains. Prime and irreducible elements. $\mathbb{Z}$ and $F[x]$ are Euclidean. Euclidean $\Rightarrow$ PID. PID $\Rightarrow$ UFD. Examples showing that each of these implications cannot be reversed (e.g., quadratic integer rings, $\mathbb{Z}[x]$, $F[x, y]$, etc.). DF 8.1 Exercises 3, 9, 10; DF 8.2 Exercises 3, 5; DF 8.3 Exercises 5–8; DF 9.1 Exercises 4–7, 9, 13; DF 9.2 Exercises 1–3, 6–7; DF 9.3 Exercises 3, 4.

**Practice exam questions:**

**1.** There will be some True/False questions covering a range of topics.

**2.** There will be some problems of the form: Given a subset of a group, determine whether it is a subgroup; given a subset of a ring, determine whether it is subring or ideal; and/or given a subset of an algebra, determine whether it is a subalgebra.

**3.** Let $p, q, r$ be prime numbers (not necessarily distinct). Depending on the values of $p, q, r$, determine the number of abelian groups of order $(pqr)^2$.

**4.** Classify all groups of order 157, 169, and 187 up to isomorphism.

**5.** Consider the subset $R$ of $M_2(\mathbb{R})$ consisting of matrices of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

Prove that $R$ is a subring of $M_2(\mathbb{R})$. Prove that $R$ is a commutative ring with 1, but is not an integral domain. Find all idempotents in $R$ (an idempotent is an element $x$ such that $x^2 = x$). Find all nilpotent elements in $R$. Define $\varphi : R \to \mathbb{R}$ by

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mapsto a - b.$$

Show that $\varphi$ is a ring homomorphism. Determine the kernel of $\varphi$ as well as $R/\ker(\varphi)$. Is $\ker(\varphi)$ a prime ideal or a maximal ideal?

**6.** Let $R = \mathbb{Z}[Z_2]$ be the group ring with coefficients $\mathbb{Z}$ associated to the cyclic group $Z_2$ of order 2. Compute the unit group $R^\times$. **Hint.** There is a multiplicative norm on this ring, by thinking about it as "$\mathbb{Z}[\sqrt{D}]$" where "$D = 1$".

**7.** Find a unit of every degree in $\mathbb{Z}/4\mathbb{Z}[x]$.

**8.** Compute the structure (invariant factors or elementary divisors) of the abelian group of homomorphisms $\mathrm{Hom}(\mathbb{Z}/36\mathbb{Z}, \mathbb{Z}/48\mathbb{Z})$ (you know how to add homomorphisms). Identify, as best you can, the rings $\mathrm{Hom}(\mathbb{Z}/36\mathbb{Z}, \mathbb{Z}/36\mathbb{Z})$ and $\mathrm{Hom}(\mathbb{Z}/48\mathbb{Z}, \mathbb{Z}/48\mathbb{Z})$ (multiplication of homomorphisms is composition).

**9.** Recall the ring $\mathbb{Z}[i]$ of Gaussian integers.

(a) Determine whether the elements 2 and 3 are irreducible.
(b) Determine whether the ideals (2) and (3) are prime or maximal.
(c) Determine whether the quotient rings $\mathbb{Z}[i]/(2)$ and $\mathbb{Z}[i]/(3)$ are integral domains. If not, find a zero-divisor.

**10.** Give an example of the following or prove that none exists:

- A Euclidean domain other than $\mathbb{Z}$ and $F[x]$.
- A PID other than $\mathbb{Z}$ and $F[x]$.
- A quotient of $\mathbb{Z}$ and $F[x]$ that is not an integral domain.
- A quotient of $\mathbb{Z}$ and $F[x]$ that is a Euclidean domain.
- A quotient of $\mathbb{Z}$ and $F[x]$ in which not every ideal is principle.
- A PID that is not Euclidean.
- A UFD that is not a PID.
- A UFD that is a Euclidean domain but is not a PID.
- An integral domain with an irreducible element that is not prime.