MA 294: Applied Abstract Algebra / Spring 2022
Some review notes for the final exam

Topics covered in the course, organized by textbook section, that may be covered on the final exam. Items marked with • are from the second half of the course; this material will be engaged in at least 2/3 of the final.

∗ Mathematical induction: section 4.3
∗ Functions: chapter 5
∗ Equivalence relations: 7.1
∗ Divisibility: sections 8.1, 8.2, 8.4, 8.5
• Permutations: section 10.6
∗ More on equivalence relations: sections 12.1, 12.2
• Cycle structure of permutations: sections 12.5
• Sign of a permutation: sections 12.6
∗ Integers modulo m, units modulo m: sections 13.1, 13.2, 13.3
∗ Groups: chapter 20, especially sections 20.1–20.8
• Lagrange's theorem: section 20.8
• Permutation groups (orbit-stabilizer formula; Burnside's lemma): sections 21.1–21.4
• Group of rotations of a tetrahedron is A_4: Example on p. 287 and Exercise 21.3.1
• Group of rotations of a cube is S_4: problems (6) and (7) on HW #8; (5) on HW #9
• Rings, fields, and polynomials: chapter 22
• Finite fields, primitive element theorem: section 23.1, 23.3, 23.4
• The RSA encryption algorithm: Judson chapter 7

Updated list of definitions. You should know all of these! One or two of these will appear as standalone questions on the final.

Solution sets to every homework problem are available on the course website and are a great study resource.

The same is true for Quiz #1, the midterm, and Quiz #2.

The course website lists every class and what was covered, with references.

The review sheet from before the midterm has some additional study problems from the first half of the course.

More problems relating to the second half of the course

(1) **Lagrange's theorem**

(a) Exercises 20.8.4 and 20.8.5
(b) Exercise 20.10.15
(c) Exercise 20.8.6. A bit of a doozy!

(d) Exercise 20.10.21. For some hints, see (6) on this old problem set.

(2) **The symmetric group and the alternating group**

(a) Write down some permutations in some S_n. Express them, their products, their powers, in cycle notation. Determine their signs.
(b) Exercise 21.7.2
(c) Exercise 21.7.4

(3) **Groups of permutations**

(a) Exercise 21.1.5
(b) Exercise 21.7.6
(c) Exercise 21.7.7 (automorphisms of the Petersen graph).

(4) **Symmetries in 3-space**

(a) The group of rotational symmetries of a cube is S_4 and the group of rotational symmetries of a tetrahedron is A_4. Inscribe two tetrahedra into a cube in such a way that half the rotational symmetries of the cube preserve each tetrahedron and half switch them. Can you see that the rotations that fix one of the tetrahedra realize all the rotational symmetries of that tetrahedron?
(b) What is the group of *all* symmetries of the tetrahedron, including those that reverse orientation (and are therefore no longer rotations in 3-space)? (Hint: it's S_4. Why?)
(c) What is the group of *all* symmetries of a cube, including those that reverse orientation? (Hint: It's $S_4 \times \mathbb{Z}_2$. Why?)
(d) Get your hands on an icosahedron (a soccer ball will do) or a dodecahedron. As with the cube/octahedron/tetrahedron, each non-identity rotational symmetry stabilizes a face or a vertex or an edge. Do the analogue of problem (6) on HW #8!

(5) **Burnside's orbit-counting lemma**

(a) Exercise 21.7.9
(b) Exercise 21.7.12
(c) Exercise 21.7.13
(d) Exercise 21.7.14
(e) Exercise 21.7.15
(f) In how many ways can the faces/vertices/edges of a tetrahedron/ cube/ octahedron/ dodecahedron/ icosahedron be painted with 2/3/4/5/6 colors? What if you're only allowed to use the first color 1/2/3/4/5 times? What if you're limited in the use of both the first and the second color?

(6) **Rings and fields**

(a) Exercise 22.1.2
(b) Exercise 22.2.1
(c) Exercise 22.9.12

(d) Exercise 22.9.13

(7) **Polynomials**

(a) Exercise 22.5.3
(b) Exercise 22.5.4
(c) Exercise 22.6.2
(d) Exercise 22.6.3
(e) Exercise 22.7.6
(f) Exercise 22.8.2
(g) Exercise 22.9.2
(h) Exercise 22.9.5
(i) Exercise 22.9.11

(8) **Finite fields and the primitive element theorem**

(a) Exercise 23.1.3
(b) Exercise 23.1.4
(c) Exercise 23.3.1
(d) Exercise 23.4.1
(e) Exercise 23.4.3 (A primitive irreducible polynomial is an irreducible polynomial $f(x)$ in $\mathbb{Z}_p[x]$ so that x is a generator of the cyclic multiplicative group of $F = (\mathbb{Z}_p[x])_{f(x)}$. This notion is useful for computations, as you may imagine — we used it when talking about the Hamming error-correcting code.)
(f) Exercise 23.4.4
(g) Exercise 23.4.5
(h) For some prime p and some irreducible polynomial $f(x)$ of degree n in $\mathbb{Z}_p[x]$, find an element of the multiplicative group of the field $F = (\mathbb{Z}_p[x])_{f(x)}$ of some particular order d. For which orders d (depending on p and on n) will you be able to do this?
(i) Exercise 23.10.1
(j) Exercise 23.10.2
(k) Exercise 23.10.3

(9) **RSA encryption**

(a) Judson exercise 7.7.
(b) Judson exercise 7.8
(c) Judson exercise 7.9
(d) Judson exercise 7.10