Abstract Algebra
Math 521A
Michael E. O'Sullivan

Review of the course

Rings and Ideals

- Know the definitions:
  - ring, commutative, identity, field;
  - unit, zero divisor, characteristic;
  - homomorphism, isomorphism.
- Know how to:
  - Prove that a subset of a ring is a subring, or an ideal (or show that it isn't).
  - Prove that a function is a homomorphism, or isomorphism (or show it isn't).
  - Show that two rings can't be isomorphic, because they have some different structure.
  - Identify the units and zero divisors in a ring.
- Know how to construct new rings from old and to compute in these rings.
  - The Cartesian product of rings R and S is a ring $R \times S$.
  - The 2×2 matrices over a ring R form a ring, which we write $M(R)$.
  - The polynomial ring, $R[x]$ over a ring R.
- Know how to work with quotient rings. (Here you may assume the ring is commutative with identity.)
  - If I is an ideal in R, the elements of R/I are written $a + I$ where $a \in R$.
  - $a + I = b + I$ when $a - b \in I$.
  - Addition in R/I is defined by $(a + I) + (b + I) = (a + b) + I$.
  - Multiplication in R/I is defined by $(a + I)(b + I) = (ab) + I$.
- Know the special properties of $\mathbb{Z}$ and $F[x]$.
  - Division theorem.
  - Euclidean algorithm.
  - Prime iff irreducible.
  - Unique factorization.
  - Every nonzero element is either a zero divisor or a unit.
  - In $F[x]$, $(x - a)$ is a factor of $f(x)$ iff a is a root of $f(x)$.
  - Any ideal in $\mathbb{Z}$, $\mathbb{Z}_n$, $F[x]$ or $F[x]/a(x)$ is principal. Be able to identify all ideals in these rings. Know how to find a generator.
  - The inverse of a unit in $\mathbb{Z}_n$ or in $F[x]/p(x)$ can be found using the Euclidean algorithm. When p is prime $\mathbb{Z}_p$ is a field. When $p(x)$ is irreducible $F[x]/p(x)$ is a field.

Groups

- Definitions
  - group, subgroup, cyclic subgroup, abelian group;
  - order of a group, order of an element;
  - homomorphism, isomorphism.
- Standard examples
  - The additive group of a ring.
  - The group of units in a ring.
  - U_n the group of units in $\mathbb{Z}_n$.
  - $Gl(2, F)$, the group of invertible 2×2 matrices over a field F.
  - $Sl(2, F)$, the group 2×2 matrices over a field F that have determinant 1.
  - D_n, the group of symmetries of a regular polygon
  - S_n the group of permutations of n objects.
- Know how to prove that a subset of a group is a subgroup (or show it is not).
- Know how to show that a group is cyclic or show it is not.
- Know how to prove that a function from group G to group H is a homomorphism.

Have a look at the last two exams and the last couple of problem sets. Here are a few extra problems:

1. Let I and J be ideals in a ring R (commutative with identity).
   (a) What is $I + J$? What is $I \times J$? What is $I \cap J$?
   (b) Show that each of these is an ideal.
2. Express in the simplest form.
   $\langle x^2 - 1\rangle + \langle x^2 + 2x + 1\rangle$ in $\mathbb{Q}[x]$.
   $\langle x^2 - 1\rangle \cap \langle x^2 + 2x + 1\rangle$ in $\mathbb{Q}[x]$.
   $\langle x^2 - 1\rangle + \langle x^2 + 2x + 1\rangle$ in $\mathbb{Q}[x]/(x^3 - 1)$.
   $\langle x^2 - 1\rangle \cap \langle x^2 + 2x + 1\rangle$ in $\mathbb{Q}[x]/(x^3 - 1)$.
3. Identify an ismorphism between $Gl(2, \mathbb{Z}_2)$ and S_3. How many isomorphisms are there? List all the subgroups of S_3
4. Show that the set of 2×2 matrices with determinant ± 1 is a subgroup of $Gl(2, F)$.
5. Show that U_{11} is a cyclic group, generated by 2. Show that U_{15} is not cyclic.