Note: to give you more flexibility in allocating your time now that the final projects are out, the following policy will be in effect for all remaining problem sets: **you can skip** 20% **of the set and still earn full points**. More precisely: when computing grades, I will reduce all scores above 80% down to 80%, and then divide by 0.8. Of course, you will still receive feedback and scores for all problems you submit, and you should think about all of the problems, since all concern material that may occur on exams. This policy is not reflected in the numbers reported on Gradescope, but it will be applied on the spreadsheet where I compute grades.

1. Let G be a group. Given any two elements $a, b \in G$, the *commutator* of a and b, denoted $[a, b]$ is defined to be
$$[a, b] = aba^{-1}b^{-1}.$$
   (a) Prove that G is abelian if and only if for all $a, b \in G$, $[a, b] = e$.
   (b) Prove that for a normal subgroup $H \triangleleft G$, the quotient group G/H is abelian if and only if $[a, b] \in H$ for all $a, b \in G$.

2. (**10.3.11**) Assume that N is a normal subgroup of a group G. Assume E is a subgroup of G/N. Thus E is a collection of right cosets of N in G. Let K be the union of all the elements of E. In other words, K is a subset of G consisting of all the elements in the right cosets in E. Prove that K is a subgroup of G that contains N. What is $|K|$?

3. Let V be a vector space, and let $W \subseteq V$ be a subspace. Regard V as an abelian group with operation $+$ (therefore W is a subgroup).
   (a) Prove that the quotient group V/W has a well-defined scalar multiplication operation, given by $c(W + \vec{v}) = W + c\vec{v}$ (this amounts to showing that the resulting coset does not depend on the coset representative $\vec{v}$). Convince yourself that V/W satisfies the axioms of a vector space (but you do not need to write anything down for this, as it's a bit tedious to check all ten axioms).
   (b) Prove that if V is finite-dimensional, then $\dim(V/W) = \dim V - \dim W$.
   Suggestion: a fact from linear algebra says that any basis $\{\vec{v}_1, \cdots, \vec{v}_m\}$ for a subspace $W \subseteq V$ may be extended to a basis $\{\vec{v}_1, \cdots, \vec{v}_n\}$ of V (you may cite this fact without proof). Show that $\{W + \vec{v}_{m+1}, \cdots, W + \vec{v}_n\}$ is a basis for V/W.
   (c) Prove that if $T : V \to U$ is a linear transformation of vector spaces, and $W = \ker T$, then the induced homomorphism $V/W \to U$ (which we know from class to be a *group* homomorphism) is a *linear transformation* of vector spaces as well.
   (d) Deduce the rank-nullity theorem (from linear algebra[1]) from the fundamental theorem of group homomorphisms (from this class).

4. Let d be a squarefree integer (positive or negative), or -1.
   (a) Prove that unit group of the ring of quadratic integers $\mathbb{Z}[\sqrt{d}]$ is given by:
$$\left(\mathbb{Z}[\sqrt{d}]\right)^\times = \{\alpha \in \mathbb{Z}[\sqrt{d}] : \ N(\alpha) = \pm 1\}.$$

[1] Your linear algebra text may have had a different name for this theorem, search for it online if this name is unfamiliar.

(b) Find an integer solution to the equation $a^2 = 5b^2 + 1$ in which both a and b are nonzero (just use trial and error). Observe that $a + b\sqrt{5}$ is a unit in $\mathbb{Z}[\sqrt{5}]$. Using the fact that the units form a group, use your first solution to find another solution in which a and b are both greater than 100.

Comment: The Diophantine equation $a^2 = db^2+1$ (for d positive and squarefree) is called *Pell's equation*; its study predates the study of rings. We now understand Pell's equation as the study of the unit group of $\mathbb{Z}[\sqrt{d}]$. The main theorem about Pell's equation is that this unit group is *cyclic*, so one can find a single small solution and use it to generate all others.

5. Call an element a of a ring R *idempotent* if $a^2 = a$ (in a ring, a^2 is shorthand for $a \cdot a$). Call a ring *Boolean* if every element is idempotent. Prove that if R is a Boolean ring, then
   (a) for all $a \in R$, $a + a = 0_R$, and
   (b) R is commutative.

   Hint for (a): consider the expression $(r + r)^2$.

6. (**15.2.1**) We know that $\mathbb{F}_3 = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ is a field. Can you find a ring with 3 elements that is not a field?

7. (**15.2.4**) Let R and S be integral domains, and let $T = R \times S$ be the direct product of R and S. Is T necessarily an integral domain? Can T ever be an integral domain?

8. (***15.2.14***) Let R be a ring with identity. Let n be a positive integer and assume that $n1 = \underbrace{1 + 1 + \cdots + 1}_{n} = 0$. Show that $nx = 0$ for every $x \in R$.

9. (**15.2.15**) Let D be an integral domain. Assume that there exists a positive integer n such that $n1 = 0$. Prove that the smallest positive integer n with $n1 = 0$ is a prime number.

10. Suppose that F is a field with four elements, labeled $\{0, 1, a, b\}$ (here $0 = 0_F$ is the additive identity and $1 = 1_F$ is the multiplicative identity). Fill out the following charts to determine the addition table and multiplication table for F. In your submission, it is not necessary to write a full formal proof that your answer is the only way to do it, but briefly summarize (in a paragraph or so) how you found the tables.

$+$	0	1	a	b
0				
1				
a				
b				

$\cdot$	0	1	a	b
0				
1				
a				
b				

Suggestion: There are many ways to proceed, so just try things out and don't be afraid of a little trial and error. A good way to start is to fill out as much as you can using basic properties of 1 and 0. After that, remember that $F^\times$ is a group, and note that the distributive property will force your hand in a number of places.

Some other good problems to try for additional practice (but not to hand in):
(I will add some problems here soon) 15.1.3, 15.1.5, 15.2.6, 15.2.7, 15.2.11, 15.2.13