189-235A: Basic Algebra I
Assignment 5

Due: Wednesday, November 28

1. Let $f : \mathbf{Z} \longrightarrow R$ be a surjective homomorphism of rings. Show that R is isomorphic either to $\mathbf{Z}$ or to the ring $\mathbf{Z}/n\mathbf{Z}$ for a suitable $n \geq 1$.

2. Let R be a commutative ring and let I be an ideal of R. Prove or disprove the statement that if R is an integral domain, then so is R/I.

3. Let $R = \mathbf{Z}[x]$, and let I be the ideal $(p, x^2 + 1)$ generated by the integer prime p and the polynomial $x^2 + 1$. Show that R/I is isomorphic to $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ is $p = 5$, and is isomorphic to a field with 49 elements if $p = 7$.

4. Let F be a field and let $R = F[[x]]$ denote the ring of formal power series with coefficients in F, i.e., the set of expressions of the form

$$\sum_{n=0}^{\infty} a_n x^n, \quad a_n \in F,$$

where the addition and multiplication are performed by formally expanding out the sums and products (without worrying about issues of convergence, which don't make sense in an arbitrary field F anyways!) Let $I = (x)$ be the ideal generated by the power series x. Show that R/I is isomorphic to F. Show that any element of R which does not belong to I is invertible. Conclude that any non-trivial ideal of R is contained in I. (A ring with this property is called a *local ring*, a terminology arising from the prototypical example $F[[x]]$, because power series can be thought of as "functions defined in an infinitesimal neighbourhood of the value $x = 0$".)

5. Let F be a field, and define a binary composition law on $G = F - \{1\}$ by the rule

$$a * b = a + b - ab.$$

Show that G, with this operation, is a group. (In particular, write down the neutral element for $*$, and give a formula for the inverse of $a \in G$.)

6. List all the elements of order 3 in S_3. How many are there?

7. Suppose that G is a group in which $x^2 = 1$, for all $x \in G$. Show that G is abelian. Give an example of a **non-abelian** group G of order 27 in which $x^3 = 1$ for all $x \in G$. (Hint: try to find such a group in the group of 3×3 invertible matrices with entries in $\mathbf{Z}/3\mathbf{Z}$.)

8. Show that the intersection of two subgroups H_1 and H_2 of a group G is a subgroup of G. What about unions of subgroups?

9. If a is an element of a finite group G of cardinality n, show that $a^n = 1$. Apply this general fact to the group $G = (\mathbf{Z}/p\mathbf{Z})^\times$ (under multiplication) to give another proof of *Fermat's Little Theorem* that p divides $a^p - a$ for all integers a when p is prime.

10. Let S be a subset of a group G. The centraliser of S, denoted $Z(S)$, is the set of $a \in G$ which commute with every $s \in S$, i.e., such that $as = sa$ for all $s \in S$. Show that $Z(S)$ is a subgroup of G.

11. Let G_1 be the group of strictly positive real numbers, under multiplication, and let G_2 be the group of all real numbers, under addition. Show that G_1 and G_2 are isomorphic, by writing down an explicit isomorphism between the two groups.

12. Recall that the *conjugacy class* of a in a group G is the set of all elements of G which are of the form gag^{-1} for some $g \in G$. Show that a normal subgroup of G is a disjoint union of conjugacy classes. List the conjugacy classes in S_4 and use this to give a complete list of all the normal subgroups of S_4. Same question for S_5.