Math 206B: Algebra
Midterm 1: Solutions

1. Describe all maximal ideals in $\mathbb{Z}/n\mathbb{Z}$ where n is a positive integer.

   Solution 1: By the Lattice Isomorphism Theorem for Rings, ideals of $\mathbb{Z}/n\mathbb{Z}$ are in bijection with ideals of $\mathbb{Z}$ that contain $n\mathbb{Z}$. Every nontrivial ideal of $\mathbb{Z}$ is of the form $k\mathbb{Z}$ for some positive integer k. We know that if a and b are positive integers then $a\mathbb{Z} \supseteq b\mathbb{Z}$ if and only if a divides b. Therefore, ideals of $\mathbb{Z}/n\mathbb{Z}$ are in bijection with ideals $m\mathbb{Z}$ where m runs through a list of divisors of n.

   For $m \mid n$, $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$, so we see that the maximal ideals of $\mathbb{Z}/n\mathbb{Z}$ are exactly those generated by $p \in \mathbb{Z}/n\mathbb{Z}$, where p is a prime divisor of n. There is one little exception, which is that if $n = p$ is a prime, then $\mathbb{Z}/n\mathbb{Z}$ is already a field and has no maximal ideals.

   Solution 2: An ideal in $\mathbb{Z}/n\mathbb{Z}$ is an additive subgroup of $\mathbb{Z}/n\mathbb{Z}$, and in fact, every additive subgroup is an ideal. Each one of these subgroups is cyclic and is generated by $\langle d \rangle$ for some positive divisor d or n. We know that $\langle a \rangle \subseteq \langle b \rangle$ if and only if a divides b. Therefore, the maximal ideals (which are the same as maximal proper subgroups) are exactly the subgroups generated by primes dividing n. There is one little exception, which is that if $n = p$ is a prime, then $\mathbb{Z}/n\mathbb{Z}$ is already a field and has no maximal ideals.

2. (a) True or False: If R is an integral domain and $I \cap J = \{0\}$ where I and J are ideals in R, then $I = \{0\}$ or $J = \{0\}$.

   Solution: This is true. Suppose that $I \neq \{0\}$ and $J \neq \{0\}$. Choose a nonzero element $a \in I$ and a nonzero $b \in J$. Since I and J are ideals, $ab \in I \cap J$. So if $I \cap J = \{0\}$ implies $ab = 0$. If R is an integral domain, then this is a contradiction.

   (b) Let R be a ring with identity $1 \neq 0$. Define the *characteristic* of R.

   Solution: The characteristic of R is the smallest positive integer n such that $1 + \cdots + 1$ (n times) is equal to 0. If no such positive integer n exists, then R has characteristic 0.

   (c) True or False: If K and L are fields and $\varphi\colon K \to L$ is a ring homomorphism that takes the identity of K to the identity of L, then K and L must have the same characteristic.

   Solution: The kernel of φ is an ideal of K. The only ideals in a field are the trivial ideal and the field itself. If $\ker(\varphi) = K$, then $\varphi(1) = 0$, so φ does not take the identity of K to the identity of L. So we now suppose that φ is injective.

   Note that

   $$\varphi(n \cdot 1_K) = \varphi(1_K) + \cdots + \varphi(1_K) = n \cdot \varphi(1_L).$$

   Now since φ is injective, we see that $\varphi(n \cdot 1_K) = 0$ if and only if $n \cdot 1_K = 0$. Therefore $n \cdot 1_K = 0$ if and only if $n \cdot 1_L = 0$. So, K and L have the same characteristic.

3. A ring R is called Noetherian if every strictly increasing chain of ideals $I_1 \subsetneq I_2 \subsetneq \cdots$ must be finite in length. Prove that if R is Noetherian, then every ideal of R is finitely generated. Prove that $\mathbb{Z}$ is Noetherian.

   Note: We proved the first part of this result in Lecture 6: Video 1.

   Solution: Let I be an ideal of R. Let $a_1 \in I$ be a nonzero element. If $(a_1) = I$, we are done. If not, choose $a_2 \in I \setminus (a_1)$. If $(a_1, a_2) = I$, then we're done. If not, choose $a_3 \in I \setminus (a_1, a_2)$. Continuing in this way, we either find a finite generating set for I or we have a chain of ideals:

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots \subsetneq I.$$

   In fact, we see that each inclusion is proper because we chose a_{i+1} so that it was not in $(a_1, \ldots, a_i)$. This is an infinite chain of ideals each properly contained in the next. This contradicts the assumption that R is Noetherian. Therefore, we must have found a finite generating set for I.

   Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some positive integer $\mathbb{Z}$. The set of ideals containing $n\mathbb{Z}$ is the set of $d\mathbb{Z}$ where d is a positive divisor of n. This set is finite, so it is clear that I_1 is only contained in finitely many ideals, and so any chain must be finite in length.

   Solution 2: For the second part, you can prove this statement without starting from the fact that every nonzero ideal of $\mathbb{Z}$ is of the form $d\mathbb{Z}$. Suppose I is a nonzero ideal of $\mathbb{Z}$. Since I is an additive subgroup it contains some positive integer. Let m be the smallest positive integer in I. We claim that any ascending chain of ideals containing I has length at most m. This is because if J is an ideal properly containing I, J must contain a positive integer smaller than m. Since $I \subsetneq J$, we see that J contains a positive integer k that is not divisible by m. Applying the division algorithm, $k = qm + r$ where $1 \leq r \leq m - 1$.

4. (a) If R is an integral domain, show that any prime element is irreducible.

   Note: This is Proposition 10 in Section 8.3.

   Solution: Suppose that $p \in R$ is prime. Therefore, (p) is a prime ideal. Suppose that $p = ab$ where $a, b \in R$ are nonzero elements. Then $ab \in (p)$. Since (p) is prime either $a \in (p)$ or $b \in (p)$. Let's suppose we are in the first case (if we're in the second case the argument is similar with a and b switched). Then $a = pr$ for some $r \in R$. Therefore, $p = ab = prb$. Since R is an integral domain, we see that $rb = 1$. Therefore b is a unit. We see that in any factorization $p = ab$ either a is a unit or b is a unit. So p is irreducible.

   (b) If R is a UFD show that any irreducible element is prime.

   Note: This is Proposition 12 in Section 8.3.

   Solution: Let $p \in R$ be an irreducible element. Consider the ideal (p). Suppose that $ab \in (p)$. Then $ab = pc$ for some $c \in R$. Since we are in a UFD, we can factor a into a finite product of irreducible elements, $a = q_1 \cdots q_r$. Similarly, we can factor b into a

finite product of irreducible elements, $b = t_1 \cdots t_s$. Since R is a UFD and $pc = ab$, we must have that p is associate to some q_i or some t_j. Switching the roles of a and b if necessary, we can suppose that p is associate to some q_i. Then p divides a.

So, whenever $ab \in (p)$, either p divides a or p divides b. Therefore, p is prime.

5. (a) Find a decomposition of 11 into a product of irreducible elements in $\mathbb{Z}[i]$.

   Solution: We know that a prime p is irreducible in $\mathbb{Z}[i]$ if and only if p cannot be written as a sum of two integer squares. Since any integer congruent to 3 modulo 4 cannot be written as a sum of two integer squares, 11 is itself irreducible in $\mathbb{Z}[i]$.

   (b) Find a decomposition of 13 into a product of irreducible elements in $\mathbb{Z}[i]$.

   Solution: Since $13 = 2^2 + 3^2$ we see that $13 = (2+3i)(2-3i)$ in $\mathbb{Z}[i]$. Since $N(2+3i) = N(2-3i) = 13$, which is prime, these elements are both irreducible in $\mathbb{Z}[i]$.

6. Suppose that I is an ideal of $R = \mathbb{Z}[x]$ and suppose that $p \in I$ for some prime number p. Prove that I can be generated by 2 elements.

   Solution: Ideals I of $\mathbb{Z}[x]$ that contain p must contain (p). We know that $\mathbb{Z}[x]/(p) \cong (\mathbb{Z}/p\mathbb{Z})[x]$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $(\mathbb{Z}/p\mathbb{Z})[x]$ is a PID. Therefore, every ideal of $(\mathbb{Z}/p\mathbb{Z})[x]$ is principal, and similarly, every ideal of $\mathbb{Z}[x]/(p) = (\overline{f})$ for some $f \in \mathbb{Z}[x]$ such that f gets sent to $\overline{f}$ by the natural projection homomorphism $\pi\colon \mathbb{Z}[x] \to \mathbb{Z}[x]/(p)$.

   We claim that $I = (p, f)$. This is because I is the set of all polynomials that reduce to something in $(\overline{f})$ after reducing coefficients modulo p. Every such polynomial can be written as $pg(x) + f(x)h(x)$ where $g(x), h(x) \in \mathbb{Z}[x]$. This is (p, f).

7. Does there exist a non-principal ideal in $\mathbb{Z}[\sqrt{-13}]$?
   Either give an example, or show that no such example exists.

   Note: This is very close to the analogous statement for $\mathbb{Z}[\sqrt{-5}]$, which is Example 2 in Section 8.1 (page 273).

   Solution: The norm in $\mathbb{Z}[\sqrt{-13}]$ is defined by $N(a + b\sqrt{-13}) = a^2 + 13b^2$. We have that

   $$14 = 2 \cdot 7 = (1 - \sqrt{-13})(1 + \sqrt{-13}).$$

   We claim that all four of the elements $2, 7, (1 - \sqrt{-13}), (1 + \sqrt{-13})$ are irreducible. It is enough to note that there are no elements in this ring of norm 2 or of norm 7. We claim that $(2, 1 - \sqrt{-13})$ is an ideal that is not principal.

   If this ideal were principal, $2, 1 - \sqrt{-13}) = (\alpha)$ for some $\alpha = a + b\sqrt{-13}$, then we would have to have $2 \in (\alpha)$ and $(1 - \sqrt{-13}) \in (\alpha)$. This would mean that $N(\alpha)$ divides $N(2)$ and $N(\alpha)$ divides $N(1 - \sqrt{-13}) = 14$. Therefore, $N(\alpha) = 2$, which is not possible, or $N(\alpha) = 1$ and this ideal is all of $\mathbb{Z}[\sqrt{-13}]$. In this case, there would be β, γ such that

   $$\beta 2 + \gamma(1 + \sqrt{-13}) = 1.$$

But then multiplying by $1 - \sqrt{-13}$ on both sides we see that

$$\beta 2(1 - \sqrt{-13}) + \gamma(1 + \sqrt{-13})(1 - \sqrt{-13}) = (1 - \sqrt{-13}).$$

The left hand side is divisible by 2, but the right hand side is not (if it were, both coefficients would be even). Therefore, $(2, 1 + \sqrt{-13}) \neq \mathbb{Z}[\sqrt{-13}]$, and $(2, 1 + \sqrt{-13})$ is not principal.

8. Let $\mathbb{Q}(x)$ be the field of fractions of the integral domain $\mathbb{Q}[x]$. For the subring

$$A = \left\{ \frac{f(x)}{g(x)} \in \mathbb{Q}(x) \colon g(0) \neq 0 \right\},$$

of $\mathbb{Q}(x)$, prove the following:

(a) A is a PID.

(b) A has a unique irreducible element up to associates.

Note: This ring is an example of a DVR, see Example (4) in Section 8.1, page 272. It is also an example of Localization, which we discussed when we talked about rings of fractions. See Example (4) in Section 15.4, page 708.

Solution: We first note that for $g(x) \in \mathbb{Q}[x]$, $g(\alpha) = 0$ if and only if x divides $g(x)$.

We know that $\mathbb{Q}[x]$ is a Euclidean domain, so it is a UFD. Any polynomial in $\mathbb{Q}[x]$ can be factored uniquely into a product of irreducible elements. Any element of A can be written as $\frac{f(x)}{g(x)}$. By factoring the numerator and denominator, we see that any element $h(x)$ of A can be written as $x^\alpha \cdot \frac{f'(x)}{g'(x)}$ where $f'(0) \neq 0$ and $g'(0) \neq 0$. By the definition of A we see that $\alpha \geq 0$.

We define a norm on A by $N(h(x)) = \alpha$. We see that the units of A are exactly the elements of norm 0. It is clear that x is irreducible, since it is irreducible in $\mathbb{Q}[x]$ and by assumption no element of A has a factor of x in its denominator. Every element of A is equal to some power of x times a unit, so x is the unique irreducible up to associates in A.

Let I be an ideal of A. Let $p(x)$ be an element of I with $N(p(x))$ minimal. We claim that $I = (p(x))$. Suppose that $q(x) \in I$. We want to show that $p(x)$ divides $q(x)$. This is clear if we write

$$p(x) = x^\alpha \frac{f'(x)}{g'(x)} \text{ where } f'(0) \neq 0 \text{ and } g'(0) \neq 0,$$

and

$$q(x) = x^\beta \frac{f''(x)}{g''(x)} \text{ where } f''(0) \neq 0 \text{ and } g''(0) \neq 0.$$

Since

$$\frac{f'(x)}{g'(x)}, \quad \frac{f''(x)}{g''(x)}$$

are units in A, we see that $p(x)$ divides $q(x)$ in A if and only if $\alpha \leq \beta$. Since $p(x)$ was chosen so that α would be minimal among all nonzero elements of A, we see that $p(x)$ divides $q(x)$.