Math 230B: Algebra
Midterm #1 Solutions
Wednesday, February 1, 2023.

Solutions

1. (a) Define Unique Factorization Domain (UFD).
   (b) Define Principal Ideal Domain (PID).
   (c) For the properties "UFD" and "PID" give an example of an integral domain that
      i. satisfies both properties,
      ii. satisfies neither property,
      iii. satisfies one property but not the other.

   Solution: An integral domain R is a UFD if every nonzero nonunit element $\alpha \in R$ can be written uniquely as a finite product of irreducible elements of R. That is, if

   $$\alpha = p_1 \cdots p_r = q_1 \cdots q_s$$

   where each p_i, q_j are irreducible, then $r = s$ and there is a way to rearrange $q_1, \ldots, q_s$ such that each q_i is associated to p_1 in R.

   An integral domain R is a PID if every nontrivial proper ideal $I \subset R$ is principal, that is, there exists $\alpha \in R$ such that $I = (\alpha)$.

   $\mathbb{Z}[i]$ is a PID that is a UFD.
   $\mathbb{Z}[\sqrt{-5}]$ is not a UFD or a PID.
   $\mathbb{Z}[x]$ is a UFD that is not a PID.

2. Factor 1300 into a product of irreducible elements in $\mathbb{Z}[i]$.

   Solution: We have $1300 = 13 \cdot 2^2 \cdot 5^2$. We have $2 = (1+i)(1-i)$. Both of these elements have norm 2, so they are irreducible. We have $5 = (1+2i)(1-2i)$. Both of these elements have norm 5, so they are irreducible. We have $13 = (2+3i)(2-3i)$. Both of these elements have norm 13, so they are irreducible. In conclusion,

   $$1300 = (1+i)^2(1-i)^2(1+2i)^2(1-2i)^2(2+3i)(2-3i).$$

3. Prove that $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible in $\mathbb{Z}[x]$.

   Solution: This polynomial has the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where $3 \mid a_0, a_1, \ldots, a_{n-1}$ but $3^2 \nmid a_0$. By Eisenstein's criterion at $p = 3$, this polynomial is irreducible.

4. Let R be a commutative ring in which every ideal is finitely generated. Prove that if there is an infinite sequence of proper ideals in R satisfying

$$I_1 \subseteq I_2 \subseteq \cdots$$

then there is some m such that $I_k = I_m$ for all $k \geq m$.

Solution: The main idea is to consider

$$I = \bigcup_{i \geq 1} I_i.$$

We claim that this an ideal of R. Suppose $a, b \in I$. Then there exists integers j, k such that $a \in I_j$ and $b \in I_k$. Without loss of generality, suppose that $j \leq k$. Since $I_j \subseteq I_k$ we see that $a \in I_k$ also. Since I_k is an ideal, $a - b \in I_k$. So $a - b \in I$ and I is an additive subgroup of R by the subgroup criterion. Let $r \in R$. Since I_j is an ideal, $ra \in I_j$. So $ra \in I$. We see that I is an ideal of R. In fact, it is a proper ideal. If $1 \in I$, then $1 \in I_k$ for some k, which contradicts the assumption that I_k is a proper ideal.

Since every ideal of R is finitely generated, I has a finite generating set $(a_1, \ldots, a_k)$. For each i, there exists an integer n_i such that $a_i \in I_{n_i}$. Let $N = \max\{n_1, \ldots, n_k\}$. Since $I_i \subseteq I_j$ for $i \leq j$, we see that each $I_{n_i} \subseteq I_N$. Therefore, $a_1, \ldots, a_k \in I_N$, so $I_N = I$. Since $I_N \subseteq I_k$ for all $k \geq N$, we see that $I_k = I_N = I$ for all $k \geq N$.

5. Let R be a PID and $\alpha \in R$ be a nonzero nonunit element.
Prove that α has at least one irreducible factor in R.

Solution: Let α be a nonzero nonunit element of R. We first show that α has one irreducible factor p. If α is irreducible, we are done. Suppose it is not. Then there exist nonunits a_1, b_1 such that $\alpha = a_1 b_1$. If either of a_1, b_1 is irreducible, we're done. If not, then there exist nonunits a_2, b_2 such that $a_1 = a_2 b_2$. If either of a_2, b_2 are irreducible, we're done. If not, we continue in this way.

We consider the chain of ideals of R : $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$. We know that each containment is strict because if $(a_1) = (a_2)$, then $a_2 \in (a_1)$, which means that there exists $\beta \in R$ with $a_2 = a_1 \beta = (a_2 b_2)\beta$. Since R is an integral domain, we must have $b_2 \beta = 1$, so a_2 is a unit.

We have an infinite chain of ideals of R. Since every ideal of R is finitely generated, this chain must stabilize. In particular, this process cannot go on forever, which means that at some point one of a_N, b_N must be irreducible.

6. (a) Determine whether the rings $(\mathbb{Z}/5\mathbb{Z})[x]/(x^2+1)$ and $(\mathbb{Z}/5\mathbb{Z})[x]/(x^2+2)$ are isomorphic.
   (b) Prove that $\mathbb{Z}[x]/(3, x^3-1)$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})[x]/(x^3-1)$.

(c) Give a complete list of the maximal ideals in the ring $(\mathbb{Z}/3\mathbb{Z})[x]/(x^3-1)$.
Explain how you know your list is complete.

Solution: We first factor the polynomials x^2+1 and x^2+2 in $(\mathbb{Z}/5\mathbb{Z})[x]$. A polynomial of degree 2 over a field is irreducible if and only if it has a root. We see that $2^2+1=0$ in $\mathbb{Z}/5\mathbb{Z}$, so $x-2$ divides x^2+1. We can check that $x^2+1=(x-2)(x-3)$ in $(\mathbb{Z}/5\mathbb{Z})[x]$. By checking each of the 5 elements of $\mathbb{Z}/5\mathbb{Z}$ we see that x^2+2 does not have any roots, which means it is irreducible over $\mathbb{Z}/5\mathbb{Z}$. Therefore, $(\mathbb{Z}/5\mathbb{Z})/(x^2+2)$ is a field. But, $(\mathbb{Z}/5\mathbb{Z})[x]/(x^2+1)$ is not an integral domain, for example $\overline{x-2}$ and $\overline{x-3}$ are nonzero elements of this ring that multiply to 0.

By the Third Isomorphism Theorem for rings, we have

$$\mathbb{Z}[x]/(3,x^3-1)\cong(\mathbb{Z}[x]/(3))/((3,x^3-1)/(3)).$$

We know that $\mathbb{Z}[x]/(3)\cong(\mathbb{Z}/3\mathbb{Z})[x]$ since (3) is the kernel of the homomorphism where we reduce each coefficient modulo 3. Note that

$$(3,x^3-1)=(3)+(x^3-1)=\{\alpha 3+\beta(x^3-1)\colon \alpha,\beta\in\mathbb{Z}[x]\}.$$

We see that $(3,x^3-1)/(3)$ is isomorphic to $(\overline{x^3-1})$ in $(\mathbb{Z}/3\mathbb{Z})[x]$ by applying the First Isomorphism Theorem for Rings to the map that takes $\alpha 3+\beta(x^3-1)$ to its reduction modulo 3.

For this part we could also consider the surjective ring homomorphism from $\mathbb{Z}[x]$ to $(\mathbb{Z}/3\mathbb{Z})[x]$ where we first reduce all of the coefficients of $f(x)$ modulo 3, which gives a polynomial in $(\mathbb{Z}/3\mathbb{Z})[x]$, and then consider the natural projection to $(\mathbb{Z}/3\mathbb{Z})[x]/(x^3-1)$. The kernel of the second map is the ideal generated by (x^3-1) is $(\mathbb{Z}/3\mathbb{Z})[x]$, so the kernel of the composition is the set of all polynomials $f(x)=3\alpha+(x^3-1)\beta$ where $\alpha,\beta\in\mathbb{Z}[x]$.

For the last part, we see that x^3-1 has 1 as a root in $(\mathbb{Z}/3\mathbb{Z})[x]$. We can factor

$$x^3-1=(x-1)(x^2+x+1)=(x-1)((x-1)(x-1))=(x-1)^3.$$

We could also have said that in a field of characteristic 3, we have $x^3-1^3=(x-1)^3$.

By the Lattice Isomorphism Theorem for Rings, ideals of $(\mathbb{Z}/3\mathbb{Z})[x]/(x^3-1)$ correspond to ideas of $(\mathbb{Z}/3\mathbb{Z})[x]$ containing (x^3-1). In $F[x]$ all ideals are principal, and we see that $(f(x))\subseteq(g(x))$ if and only if $g(x)\mid f(x)$. So the only ideals of $(\mathbb{Z}/3\mathbb{Z})[x]$ that contain (x^3-1) are $(\mathbb{Z}/3\mathbb{Z})[x]$, $(x-1)$, $((x-1)^2)$, and $((x-1)^3)$. In $F[x]$ an ideal is maximal if and only if it is prime and $(g(x))$ is prime if and only if $g(x)$ is irreducible. Therefore, the only one of these ideals that is maximal is $(x-1)$.

7. Let $R=\mathbb{Z}/n\mathbb{Z}$ where n is a positive integer. Is it necessarily true that a polynomial $f(x)\in R[x]$ with degree d has at most d distinct roots in R?
Explain your answer.

Solution: This is not necessarily true. Consider $n=8$ and the polynomial x^2-1. This has 4 roots, $\{1,3,5,7\}$.

8. Prove that $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

Solution: We have $10 = 2 \cdot 5 = (\sqrt{10})^2$. We claim that $5, \sqrt{10}$ are all irreducible elements in this ring and that 2 and 5 are not associate to $\sqrt{10}$.

We first show that there are no elements of $\mathbb{Z}[\sqrt{10}]$ of norm ± 5. We recall the norm on $\mathbb{Q}(\sqrt{10})$ given by $N(a + b\sqrt{10}) = a^2 - 10b^2$. This norm is multiplicative and $a + b\sqrt{10}$ is a unit if and only if its norm is 1 or -1. We have $N(5) = 25$. So if $5 = \alpha\beta$ with both α, β nonunits, then we must have $N(\alpha) = \pm 5$. We will show that there are no elements of $\mathbb{Z}[\sqrt{5}]$ of norm ± 5.

Suppose $a^2 - 10b^2 = \pm 5$. Since $-10b^2$ and ± 5 are divisible by 5, we see that $5 \mid a$. Write $a = 5a'$. This gives $25(a')^2 - 10b^2 = 5$, so $5(a')^2 - 2b^2 = \pm 1$. Taking this equation modulo 5 gives $3b^2 \equiv \pm 1 \pmod{5}$. This has no solutions modulo 5.

Therefore, 5 is irreducible in $\mathbb{Z}[\sqrt{10}]$. We see that $\sqrt{10}$ is irreducible also, since $N(\sqrt{10}) = -10$. If we did have $\sqrt{10} = \alpha\beta$ with α, β nonunits, then one of α, β would have norm ± 5 and the other would have norm ± 2. Since there are no elements of norm ± 5, this is impossible.

Therefore, $10 = \sqrt{10} \cdot \sqrt{10}$ is a factorization into irreducibles. No matter how 2 factors into a product of irreducibles (it is irreducible, but you don't need that here), we have a factorization of 10 into irreducibles that contains 5. It is clear that 5 is not associate to $\sqrt{10}$ because these elements have different norms. We conclude that $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

Note: There are other ways to do this. For example, you can do the same idea with the factorizations:

$$-9 = (-3) \cdot 3 = (1 - \sqrt{10})(1 + \sqrt{10}).$$

We claim that the elements $3, 1 + \sqrt{10}, 1 - \sqrt{10}$ are all irreducible. This follows from the fact that there are no elements of norm ± 3. This is because $a^2 - 10b^2 = \pm 3$ has no integer solutions. The easiest way to see this is the reduce this equation modulo 5 to get $a^2 \equiv \pm 3 \pmod{5}$, which has no solutions. (You could so something similar if you reduce modulo 10.) We see that 3 is not associate to either $1 + \sqrt{10}$ or $1 - \sqrt{10}$ by taking the quotient in $\mathbb{Q}(\sqrt{10})$ and seeing that it is not in $\mathbb{Z}[\sqrt{10}]$. Several people tried to say that the only units in $\mathbb{Z}[\sqrt{10}]$ are ± 1, but this is not true! This ring has infinitely many units. For example, $3 - \sqrt{10}$ has norm -1, so it is a unit.

Finally, a few people tried to show that there are no elements of norm ± 2, which implies that 2 is irreducible (and gives a different argument that $\sqrt{10}$ is irreducible. The easiest way to show that this is true is to take the equation $a^2 - 10b^2 = \pm 2$ modulo 5 or modulo 10 and see that is has no solutions.