Math 206B: Algebra
Midterm 2 Solutions
Friday, February 26, 2021.

Solutions

1. Let F be a field and $f(x) \in F[x]$.
   Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

   Solution: $F[x]$ is a Euclidean domain, so it is a PID. In a commutative ring R, the quotient R/M is a field if and only if M is maximal. Therefore, we need only show that $(f(x))$ is maximal if and only if $f(x)$ is irreducible.

   In an integral domain, prime elements are always irreducible. If $f(x)$ is reducible, then $(f(x))$ is not prime, so $(f(x))$ is not maximal.

   In a PID every irreducible element is prime and every prime ideal is maximal. Therefore, if $f(x)$ is irreducible then $(f(x))$ is a maximal ideal.

2. (a) Let R be a ring with a 1. Give the definition of a unital left R-module.
   Solution: A left R-module M is a set together with a binary operation $+$ that makes M into an abelian group, and an action of R on M satisfying:
      i. $r \cdot (s \cdot m) = (rs) \cdot m$ for all $r, s \in R,\ m \in M$;
      ii. $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r \in R,\ m, n \in M$;
      iii. $(r + s) \cdot m = r \cdot m + s \cdot m$ for all $r, s \in R,\ m \in M$;
      iv. $1 \cdot m = m$ for all $m \in M$.

   (b) Define what it means for a left R-module M to be free on a subset $A \subseteq M$.
   Solution: M is free on A if for every nonzero element $x \in A$ there are unique nonzero $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n \in A$ such that
   $$x = r_1 \cdot a_1 + \cdots + r_n \cdot a_n$$
   for some positive integer n.
   Equivalently, M is free on A if
   $$\sum_{i=1}^{n} r_i \cdot a_i = 0$$
   implies that all r_i are equal to 0.

   (c) Let M and N be R-modules.
   Define what it means for a map $\varphi :\ M \to N$ to be an R-module homomorphism.
   Solution: φ is an R-module homomorphism if and only if it satisfies

i. $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$;

ii. $\varphi(r \cdot x) = r \cdot \varphi(x)$ for all $r \in R$ and $x \in M$.

(d) Suppose M and N are both R-modules and that both M and N are rings.
Give an example of a map $\varphi\colon M \to N$ that is an R-module homomorphism but not a ring homomorphism.

Solution: Let $R = \mathbb{Z}$ and consider the $\mathbb{Z}$-modules $M = N = \mathbb{Z}$. We know $\mathbb{Z}$ is a ring. We know that $\mathbb{Z}$-module homomorphisms are just homomorphisms of abelian groups. The $\mathbb{Z}$-module homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(x) = 2x$ is not a ring homomorphism because

$$2 = \varphi(1 \cdot 1) \neq \varphi(1) \cdot \varphi(1) = 2 \cdot 2 = 4.$$

3. **State whether the following claim is true or false. No Explanation is Necessary.**

Suppose R is an *integral domain*.
If $f(x) \in R[x]$ has degree d, then $f(x)$ has at most d distinct roots in R.

Solution: This is true. Let F be the field of fractions of R. We show that $f(x)$ has at most d distinct roots in R by showing that $f(x)$ has at most d distinct roots in F.

This follows from the fact that a polynomial in $F[x]$ has a root in F if and only if it has a factor of degree 1. Now, $F[x]$ is a UFD. The total number of distinct roots of a polynomial $f(x)$ in F is at most the number of linear factors in the (unique) factorization of $f(x)$. The result follows by induction on the degree.

4. All of the following are isomorphic as $\mathbb{R}$-vector spaces, but only two of the following are isomorphic as rings. Which two?
Explain why they are isomorphic as rings.

(a) $\mathbb{C} \times \mathbb{C}$
(b) $\mathbb{C}[x]/(x^2)$
(c) $\mathbb{C}[x]/(x^2+1)$
(d) $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$
(e) $\mathbb{R}[x]/(x^4)$

Solution: We know that if F is a field and $f(x) \in F[x]$, then

$$F[x]/(f(x)) \cong F[x]/(g_1(x)^{r_1}) \times \cdots \times F[x]/(g_n(x)^{r_n})$$

where $f(x) = ug_1(x)^{r_1} \cdots g_n(x)^{r_n}$ is factorization of $f(x)$ (in the UFD $F[x]$) and $g_1(x), \ldots, g_n(x)$ are distinct monic irreducibles in $F[x]$, and each $r_i \geq 1$.

We note that $x^2+1 = (x+i)(x-i)$ in $\mathbb{C}[x]$, and therefore

$$\mathbb{C}[x]/(x^2+1) \cong \mathbb{C}[x]/(x+i) \times \mathbb{C}[x]/(x-i) \cong \mathbb{C} \times \mathbb{C}.$$

This last statement follows from the fact that $\varphi \colon \mathbb{C}[x] \to \mathbb{C}$ defined by $\varphi(f(x)) = f(i)$ is a surjective homomorphism with kernel $(x - i)$ (and the corresponding statement for $\varphi(f(x)) = f(-i)$).

5. What are all of the maximal ideals in the ring $\mathbb{Q}[x]/(x^3 + x^2)$?
   Explain how you know that this is a complete list.

   Solution: Let F be a field. By the Lattice Isomorphism Theorem for Rings, there is a bijection between ideals in $F[x]/(f(x))$ and ideals in $\mathbb{F}[x]$ containing $(f(x))$. Since $F[x]$ is a PID, we see that $(g(x))$ contains $(f(x))$ if and only if $g(x)$ divides $f(x)$ in $F[x]$.

   Since $x^3 + x^2 = x^2(x + 1)$ in $\mathbb{Q}[x]$, we see that the proper ideals in $\mathbb{Q}[x]$ containing $x^3 + x^2$ are exactly $(x), (x^2), (x(x + 1))$, and $(x + 1)$. The maximal ones are the ones corresponding to the irreducible polynomials, (x) and $(x + 1)$. Therefore, there are two maximal ideals in $\mathbb{Q}[x]/(x^3 + x^2)$, which are $(x)/(x^3 + x^2)$ and $(x + 1)/(x^3 + x^2)$.

6. **Prove** that the polynomial $x^4 + 15x^3 + 20x^2 + 10x + 45$ is irreducible over $\mathbb{Q}$.

   Solution: Since this is a monic polynomial and 5 divides every coefficient (except the leading 1), and 5^2 does not divide 45, this polynomial is irreducible by applying Eisenstein's criterion at $p = 5$.

7. For which primes p is the quotient $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + x + 1)$ a field?
   Prove that your answer is correct.

   Solution: We see that this quotient is a field if and only if $x^2 + x + 1$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$. Since this polynomial has degree 2, it is irreducible if and only if it does not have a root in $\mathbb{Z}/p\mathbb{Z}$. We see that 1 is a root of this polynomial if and only if $p = 3$. In all other cases, since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, a root of $x^2 + x + 1$ corresponds to an element in $\mathbb{Z}/p\mathbb{Z}^*$ of order 3. Since $|\mathbb{Z}/p\mathbb{Z}^*| = p - 1$, we see that $\mathbb{Z}/p\mathbb{Z}^*$ has an element of order 3 if and only if $p \equiv 1 \pmod 3$. Therefore, this quotient is a field if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

8. Let $G = \mathbb{Z}/25\mathbb{Z}$ the cyclic **group** of order 25.
   Can G be given the structure of a (unital) $\mathbb{Z}/5\mathbb{Z}$-module?
   Explain your answer.

   Solution: Suppose G can be given the structure of a unital $\mathbb{Z}/5\mathbb{Z}$-module. We must have $1 \cdot 1 = 1$ and we must also have

   $$0 = 0 \cdot 1 = (1 + 1 + 1 + 1 + 1) \cdot 1 = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1.$$

   This is a contradiction since $0 \neq 5$ in G.

   To say this a different way, a $\mathbb{Z}/5\mathbb{Z}$-module is a vector space over $\mathbb{Z}/5\mathbb{Z}$, and the abelian group $\mathbb{Z}/5^2\mathbb{Z}$ is not. (In a vector space over $\mathbb{Z}/5\mathbb{Z}$ every element has additive order dividing 5.)

9. (a) Does there exists a ring R with identity and an R-module M such that M is torsion-free and no linearly independent subset generates M?

Solution: Let $M = \mathbb{Q}$. This is a $\mathbb{Z}$-module since it is an abelian group. It is torsion free since $n \cdot \frac{a}{b} = 0$ implies $n = 0$ or $\frac{a}{b} = 0$. Any subset of M of size 2 or greater is linearly dependent. Let $\frac{a}{b}$, $\frac{c}{d} \in \mathbb{Q}$. If either one is zero, it is easy to see that this set is linearly dependent. So $a, b, c, d \neq 0$. Then we have a nontrivial linear relation

$$bc \cdot \frac{a}{b} - ad \cdot \frac{c}{d} = 0.$$

No set of size 1 spans $\mathbb{Q}$. The set of $\mathbb{Z}$-linear combinations of $\frac{a}{b}$ only contains rational numbers with denominators of at most b. Therefore, no linearly independent subset generates M.

Note: In lecture we gave another example that works here:

$$R = \mathbb{Z}[\sqrt{-5}],\ I = (2, 1 + \sqrt{-5}).$$

(b) Does there exists a ring R with identity and an R-module M such that M is free, $A \subseteq M$ is a maximal linearly independent set, but A does not generate M?

Solution: Let $M = \mathbb{Z}$. This is a free $\mathbb{Z}$-module: $\{1\}$ is a basis. The set $\{2\}$ is a maximal linearly independent set that does not generate $\mathbb{Z}$. We need only note that for any integer x, $\{2, x\}$ satisfies the nontrivial linear relation $-2 \cdot x + 2 \cdot x = 0$, so $\{2, x\}$ is linearly dependent.

Note: There are many other examples that work for both parts here.