Math 206B: Algebra

Final Exam Solutions

Thursday, March 18, 2021.

True/False and Short Answer

1. True or False: If R is a commutative ring with identity and R has a unique prime ideal then R is a field.
   Solution: This is false. For example, consider the subring of $\mathbb{Q}$ consisting of all rational numbers with odd denominators. This has a unique prime ideal, (2).
   We saw another example of such a ring on Midterm 1.

2. True or False: Let R be a PID, M be a finitely generated free R-module, and N be a submodule of M. Then N is free.
   Solution: This is true. This is part of the main theorem we used in proving the Classification of Modules over a PID, Existence: Invariant Factor Form.
   (Theorem 4 in Section 12.1 of Dummit and Foote.)

3. True or False: Let R be an integral domain, M be a finitely generated R-module and N be a submodule of M. Then N is finitely generated.
   There was a typo in this question. Everyone will receive full credit for it.
   Solution: This is false. Let R be a ring that has an ideal I that is not finitely generated. R is a module over itself and I is a submodule that is not finitely generated.

4. True or False: Let V be a vector space and $V = A \oplus B = C \oplus D$ with $A \cong C$. Then $B \cong D$.
   Solution: When V is infinite dimensional it is not always true that $B \cong D$. For example, suppose $A = \bigoplus_{i=1}^{\infty} F$ and $B = F$ and $D = F^2$. Then we have $A \oplus B \cong C \oplus D$, but $B \not\cong C$.
   (Two free F-modules on sets of the same cardinality are isomorphic– Exercise 1 Section 10.3.)

5. Is there an example of a UFD that is not a PID?
   Solution: Yes– $\mathbb{Z}[x]$ is a UFD that is not a PID. We know that $\mathbb{Z}$ is a UFD and that if R is a UFD then $R[x]$ is a UFD. We know that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is an integral domain that is not a field. Therefore (x) is a prime ideal that is not maximal, so $\mathbb{Z}[x]$ cannot be a PID.

6. Let $\mathbb{F}_3$ be a finite field of order 3. Let V be a 3-dimensional vector space over $\mathbb{F}_3$. How many 2-dimensional subspaces are contained in V?
   Solution: Let F be a finite field of size q and V and n-dimensional vector space over F.
   We know that the number of k-dimensional subspaces of V is

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

In this case we get

$$\frac{(27-1)(27-3)}{(9-1)(9-3)} = \frac{26 \cdot 24}{8 \cdot 6} = 13.$$

1 Problems

1. Let V, U, and W be finite dimensional vector spaces over $\mathbb{C}$. Suppose that $\phi\colon V \to U$ is an injective linear transformation and $\psi\colon U \to W$ is a surjective linear transformation.
   Suppose that $\psi \circ \phi = 0$ and that $\dim U = \dim V + \dim W$.
   Prove that $\ker(\psi) = \mathrm{Im}(\phi)$ as subspaces of U.

   Solution: Let $v_1, \ldots, v_n$ be a basis for V. Then $\phi(V)$ is isomorphic to V and $\phi(v_1), \ldots, \phi(v_n)$ is a basis for it. We know that this can be extended to a basis of U : $\phi(v_1), \ldots, \phi(v_n), u_1, \ldots, u_k$.

   Since $\dim U = \dim V + \dim W$ we see that $\dim W = k$. Applying the surjective map ψ to our basis vectors for U we see that $\psi(\phi(v_1)), \ldots, \psi(\phi(v_n)), \psi(u_1), \ldots, \psi(u_k)$ is a generating set for W. Since $\psi \circ \phi = 0$ we see that $\psi(\phi(v_1)) = \cdots = \psi(\phi(v_n)) = 0$. Therefore, $\psi(u_1), \ldots, \psi(u_k)$ is a generating set of W of size k, so it is a basis for W. In particular, no nonzero linear combination of $u_1, \ldots, u_k$ is in $\ker(\psi)$.

   We conclude that $\ker(\psi)$ is exactly equal to the subspace of U generated by $\phi(v_1), \ldots, \phi(v_n)$. We saw earlier that these vectors are a basis for the image of ϕ.

2. Let R be a PID and let M be a finitely generated R-module.
   Describe the structure of $M/\operatorname{Tor}(M)$.

   Solution: By the classification of finitely generated R-modules, we have that

   $$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

   where $a_1, \ldots, a_m$ are nonzero nonunit elements of R satisfying $a_1 \mid a_2 \mid \cdots \mid a_m$.
   We know that

   $$\operatorname{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_m).$$

   We have a natural projection homomorphism $\pi\colon M \to R^r$ by first applying the isomorphism described above and then taking

   $$\pi(x_1, \ldots, x_r, y_1 \mod (a), \ldots, y_m \mod (a_m)) = (x_1, \ldots, x_r).$$

   It is clear that π is surjective and $\ker(\pi) \cong \operatorname{Tor}(M)$.
   Applying the 1st Isomorphism Theorem completes the proof.

3. Let R be a ring and let M be a left R-module. Let

$$M_1 \subseteq M_2 \subseteq \cdots$$

be a chain of submodules of M. Let

$$N = \bigcup_{i=1}^{\infty} M_i.$$

Prove that N is a submodule of M.

Solution: We apply the submodule criterion: N is a submodule if and only if for all $x, y \in N$ and $r \in R$ we have $x + r \cdot y \in N$.

Suppose $x, y \in N$. Then $x \in M_i$ for some i and $y \in M_j$ for some j. Without loss of generality, $j \geq i$. So $x, y \in M_j$. Since M_j is a submodule of M, by the submodule criterion $x+r\cdot y \in M_j$. Therefore $x + r \cdot y \in N$.

4. Let R be a commutative ring with 1 and M be any R-module. Prove that $R \otimes_R M \cong M$.

Solution: We claim that the map $r \otimes m \to m$ is an R-module isomorphism.

We know that the map $R \times M \to M$ given by $(r, m) \to r \cdot m$ is bilinear (this is basically the definition of what it means for M to be an R-module). By the universal mapping property for tensor products there exists a unique linear map $L \colon R \otimes_R M \to M$ for which $L(r \otimes m) = rm$. We claim that this R-module homomorphism is injective and surjective. It is surjective since $L(1 \otimes m) = m$. Every element of $R \otimes_R M$ is a finite sum of elementary tensors,

$$\sum_{i=1}^{n} (r_i \otimes m_i) = \sum_{i=1}^{n} (1 \otimes r_i m_i).$$

If

$$L\left(\sum_{i=1}^{n} (1 \otimes r_i m_i\right) = \sum_{i=1}^{n} r_i m_i = 0$$

then $\sum_{i=1}^{n} r_i m_i = 0$, and $\sum_{i=1}^{n} (r_i \otimes m_i) = 0$. So this map is injective.

I will also point out that several people proved this result (and in particular the injectivity part) by showing that $f \colon M \to R \otimes_R M$ defined by $f(m) = 1 \otimes m$ is a two-sided inverse for L. This is the strategy Conrad uses in the proof of Theorem 4.5 in his 'Tensor Products' notes. (This statement is the special case where $I = 0$.)

5. Suppose A is a finite abelian group, S is a Sylow p-subgroup of A, and p^k is the order of S. Prove that $\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A$ is isomorphic to S.

Solution: Let $|A| = n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where the p_i are distinct primes. By the classification of finite abelian groups,

$$A \cong B_1 \oplus \cdots \oplus B_k$$

where B_i is a finite abelian group of order $p_i^{\alpha_i}$. Moreover, each B_i can be written as a direct sum of cyclic $\mathbb{Z}$-modules of prime power order,

$$B_i \cong \mathbb{Z}/p_i^{\beta_{i,1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_i^{\beta_{i,r_i}}\mathbb{Z}.$$

We know that

$$\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A \cong (\mathbb{Z}/p^k\mathbb{Z} \oplus B_1) \oplus \cdots (\mathbb{Z}/p^k\mathbb{Z} \oplus B_k).$$

Then

$$(\mathbb{Z}/p^k\mathbb{Z} \oplus B_i) \cong \mathbb{Z}/\gcd(p^k, p_i^{\beta_{i,1}})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\gcd(p^k, p_i^{\beta_{i,r_i}})\mathbb{Z}.$$

If $p \neq p_i$, then this group is trivial. If $p = p_i$ then $p^k = |B_i|$ and $\gcd(p^k, p_i^{\beta_{i,j}}) = p_i^{\beta_{i,j}}$. We conclude that this group is isomorphic to B_i, the Sylow p-subgroup of A.

I will also point out that several people used the fact from Example 4.6 in Conrad's 'Tensor Products' notes that $\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A/p^k Z$. But, then you need to show that $A/p^kA \cong S$. One way to do this is to consider the map $[p^k]\colon A \to A$ defined by $[p^k](x) = x + \cdots + x$ (p^ktimes). By definition, the image is p^kA. It is also clear that $x \in \ker([p^k])$ if and only if the order of x divides p^k. The elements in a finite abelian group whose order divides $|S|$ are exactly the elements of the Sylow p-subgroup S. This shows that p^kA is the set of elements in $A \setminus S$ together with 0. So we can write $A \cong S \times p^kA$ and consider the projection onto S, that is, $\pi(a, b) = a$. The kernel is p^kA.

6. For which values of $a \in \mathbb{Z}/5\mathbb{Z}$ is the ring $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3 + ax + 2)$ a field?
   Solution: This is equivalent to asking for the values of a for which $x^3 + ax + 2$ has no roots in $\mathbb{Z}/5\mathbb{Z}$. A cubic polynomial over a field F is irreducible if and only if it has no roots in F.

   We work backwards and determine the values of a for which each of the elements of $\mathbb{Z}/5\mathbb{Z}$ is a root. We see that 0 is a root if and only if $2 = 0$, that 1 is a root if and only if $3 + a = 0$, which means $a = 2$, that 2 is a root if and only if $3 + 2a + 2 = 0$, which means $a = 0$, that 3 is a root if and only if $-1 + 3a = 0$, which means $a = 2$, and that 4 is a root if and only if $-a + 1 = 0$, which means that $a = 1$.

   We conclude by noting that when $a = 0, 1, 2$ this polynomial has a root and if $a = 3, 4$ this polynomial does not have a root.

7. Prove that a finite subgroup of the multiplicative group of a field is cyclic.

   Solution: Let G be a finite subgroup of F^*. By the Classification of Finite Abelian Groups,

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z},$$

where each $n_j \geq 2$ and $n_{i+1} \mid n_i$ for each $i \in \{1, \ldots, t-1\}$. We show that $t = 1$, which implies that G is cyclic.

An element of order dividing n_t in G is an element of order dividing n_t in F^*, which is a root of the polynomial $x^{n_t} - 1$ in $F[x]$. A polynomial of degree n_t in $F[x]$ has at most n_t distinct roots in F.

In the subgroup of G given by the last factor in the decomposition above, we have n_t elements of order dividing n_t. We also have n_t elements of order dividing n_t in each of the other factors, since n_t divides n_j for each $j \leq t$. Therefore, if $t \geq 2$, then G has too many elements of order dividing n_t. So $t = 1$.

8. Find the greatest common divisor $d(X)$ of the polynomials

$$f(X) = X^4 - X^2 + 2X - 1, \quad \text{and } g(X) = X^4 + 2X^3 + X^2 - 1$$

in $\mathbb{R}[X]$.

Solution: We apply the Division Algorithm and see that

$$(X^4 - X^2 + 2X - 1) = 1 \cdot (X^4 + 2X^3 + X^2 - 1) + (-2X^3 - 2X^2 + 2X).$$

We apply the Division Algorithm again and see that

$$(X^4 + 2X^3 + X^2 - 1) = \left(\frac{-1}{2}X - \frac{1}{2}\right)(-2X^3 - 2X^2 + 2X) + (X^2 + X - 1).$$

We apply the Division Algorithm again and see that

$$(-2X^3 - 2X^2 + 2X) = (-2X) \cdot (X^2 + X - 1) + 0.$$

Since $X^2 + X - 1$ is the last nonzero remainder in this process, it is $\gcd(f(X), g(X))$.

9. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Solution: We see that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and claim that each of $2, 3, 1 \pm \sqrt{-5}$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$ and that no two of these are associate.

In $\mathbb{Z}[\sqrt{-5}]$ we have the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$ and we know that α is a unit if and only if $N(\alpha) = \pm 1$. Therefore, the only units are ± 1. So it is clear that no two of these elements are associate. We note that this norm takes only nonnegative values.

We see that $N(2) = 4,\ N(3) = 9$, and $N(1 \pm \sqrt{-5}) = 6$. Since the norm is multiplicative, showing that there are no elements of $\mathbb{Z}[\sqrt{-5}]$ of norm 2 and no elements of norm 3, shows that $2, 3$, and $1 \pm \sqrt{-5}$ are irreducible.

We see that $x^2 + 5y^2 = 2$ has no integer solutions (note that $y^2 \geq 0$ and 2 is not a square), and similarly that $x^2 + 5y^2 = 3$ has no solutions.