E. Dummit's Math 5111 ∼ Algebra 1, Fall 2020 ∼ Homework 2, due Fri Sep 25th.

Justify all responses with proof and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers.

---

1. Let R be a ring with 1. We say R is a simple ring if the only two-sided ideals of R are 0 and R.
   (a) Show that a commutative simple ring is a field.
   (b) Show that any division ring is a simple ring.
   (c) If F is a field, show that $M_{n\times n}(F)$ is a simple ring. [Hint: If I is an ideal and $A \in I$ is nonzero, by multiplying A on the left and right by matrices having only a single nonzero entry, and adding some of the results, show that the identity matrix must be in I.]
   (d) Suppose $\varphi : R_1 \to R_2$ is a surjective homomorphism and R_1, R_2 are simple rings. Show that φ is an isomorphism.

---

2. Let R be a ring.
   (a) Show that there exists a ring homomorphism $\psi : \mathbb{Z} \to R$ with $\psi(1) = r$ if and only if $r^2 = r$.
   (b) If R is an integral domain, deduce that there are exactly two ring homomorphisms from $\mathbb{Z}$ to R.
   (c) Find all of the ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/24\mathbb{Z}$.

---

3. Suppose $\varphi : R \to S$ is a ring homomorphism. If A is a subset of S, then we define the inverse image of A under φ to be the set $\varphi^{-1}(A) = \{r \in R : \varphi(r) \in A\}$ of elements of R mapped into A by φ.
   (a) If J is an ideal of S, show that $\varphi^{-1}(J)$ is an ideal of R.
   (b) If R is a subring of S and J is an ideal of S, show that $J \cap R$ is an ideal of R. [Hint: Use part (a) for a particular φ.]
   (c) If φ is surjective and I is an ideal of R, show that $\varphi(I)$ is an ideal of S.
   (d) Show that if φ is not surjective and I is an ideal of R, then $\varphi(I)$ need not necessarily be an ideal of S.
   (e) If φ is surjective and J is an ideal of S, show that $R/\varphi^{-1}(J)$ is isomorphic to S/J.

---

4. Solve:
   (a) Show that the set $\{11,\ 19 + 3i,\ e + \pi i\}$ is a spanning set for $\mathbb{C}$ over $\mathbb{R}$, but is not linearly independent.
   (b) Show that the set $\{\sqrt{2}, \sqrt{-3}\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.
   (c) If D is a squarefree integer, find a basis for $\mathbb{Q}(\sqrt{D})$ and compute $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{D})$.

---

5. Let F be a field. Suppose V is an F-vector space and that the set $\{v_1, v_2, v_3\}$ is a basis for V over F. Prove that $S = \{v_1 + v_2, v_1 + v_3, v_2 + v_3\}$ is also a basis for V over F if and only if the characteristic of F is not equal to 2.

---

6. Let F be a field, d be a positive integer, and take V to be the F-vector subspace of $F[x]$ consisting of the polynomials of degree at most d.

   (a) Find a basis for V and determine $\dim_F V$.

   Now let $a_0, a_1, \dots, a_d$ be distinct elements of F, and consider the linear transformation $T : V \to F^{d+1}$ given by $T(p) = (p(a_0), p(a_1), \dots, p(a_d))$.

   (b) Show that $T(p) = \mathbf{0}$ only for $p = 0$, and conclude that $\ker(T) = \{0\}$.

   (c) Show that that T is an isomorphism of vector spaces. [Hint: Use the nullity-rank theorem.]

   (d) Conclude that, for any list of $d+1$ points $(a_0, b_0), \dots, (a_d, b_d)$ in F^2 with distinct first coordinates, there exists a unique polynomial of degree at most d in $F[x]$ having the property that $p(a_i) = b_i$ for each $0 \le i \le d$.

---

7. Let F be a field. Suppose $p \in F[x]$ has positive degree. Show that there exists a nonzero polynomial $q(x) \in F[x]$ such that every monomial term in the product $p(x)q(x)$ has a prime exponent. (For example, for $p(x) = 2x^2 + x + 2$, the polynomial $q(x) = 2x^5 - x^4 + x^2$ works, since $p(x)q(x) = 2x^2 + x^3 + 3x^5 + 4x^7$.)

---

8. Suppose F is a finite field. Show that F must have positive characteristic p, and in fact that the number of elements in F must be a prime power.

   - Remark: We will later prove the converse of this result; namely, that for any prime power there exists a finite field having that number of elements.
