Problem Set 2 (Due Friday September 20)

Please see the course website for policy regarding collaboration and formatting your homework.

(12) In Homework Problem 8, you gave a bijection between isomorphism classes of $k[t]$ modules and pairs (V, T) with V a k-vector space and T a k-linear endomorphism.
  (a) Let $M = k[t]/(t^3 - 2)k[t]$. Give an explicit 3×3 matrix for the corresponding T.
  (b) Do $(\mathbb{R}^2, \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right])$ and $(\mathbb{R}^2, \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right])$ correspond to isomorphic $\mathbb{R}[t]$ modules or not?

(13) Let $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ be a monic irreducible polynomial with coefficients in $\mathbb{Z}$. Let θ be a root of $f(x)$ in $\mathbb{C}$ and let $\mathbb{Z}[\theta]$ be the subring of $\mathbb{C}$ generated by θ.
  (a) Show that $\mathbb{Z}[x]/f(x)\mathbb{Z}[x] \cong \mathbb{Z}[\theta]$.
  (b) Show that $\mathbb{Z}[\theta]$ is a free $\mathbb{Z}$-module with basis $1, \theta, \ldots, \theta^{n-1}$. In other words, show that every element of $\mathbb{Z}[\theta]$ can be written in the form $\sum_{j=0}^{n-1} a_j \theta^j$ for $a_j \in Z$ in precisely one way.
  (c) Let $R_3 = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ and $R_7 = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$. Show that $R_3/2R_3$ is a field with four elements and that $R_7/2R_7 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(14) Let R be a commutative ring. Let S be a subset of R which is closed under multiplication and such that[1], for $s \in S$ and $r \in R$, if $sr = 0$ then $r = 0$. Define a relation $\sim$ on $S \times R$ by $(s, r) \sim (s', r')$ if $sr' = s'r$.
  (a) Show that $\sim$ is an equivalence relation.

  Let $S^{-1}R$ be the set of equivalence classes for $\sim$ and write $s^{-1}r$ for the class of (s, r) in $S^{-1}R$. Define:

$$s_1^{-1}r_1 + s_2^{-1}r_2 = (s_1 s_2)^{-1}(s_2 r_1 + s_1 r_2) \qquad (s_1^{-1}r_1) \times (s_2^{-1}r_2) = (s_1 s_2)^{-1}(r_1 r_2).$$

  (b) Show that these operations are well-defined maps $S^{-1}R \times S^{-1}R \longrightarrow S^{-1}R$.
  (c) Show that $(S^{-1}R, +, \times)$ is a commutative ring.

  If R is an integral domain, and $S = R \setminus \{0\}$, then $S^{-1}R$ is called the ***field of fractions*** of R, and denoted $\mathrm{Frac}(R)$.

(15) Let R be a commutative ring. R is called ***local*** if R has precisely one maximal ideal. Show that a ring A is local if and only if the set of non-units in A forms an ideal of A.

(16) For two elements u and v in a ring R, will write uRv for $\{urv : r \in R\}$. Let e be idempotent in R; recall that this means $e^2 = e$. Recall that an element z of R is called central if $zr = rz$ for all $r \in R$.
  (a) Show that $1 - e$ is idempotent.
  (b) Show that, as abelian groups under the operation $+_R$, we have

$$R = eRe \,\oplus\, eR(1-e) \,\oplus\, (1-e)Re \,\oplus\, (1-e)R(1-e).$$

  (c) Suppose that e is a central idempotent. Show that $R \cong eRe \times (1-e)R(1-e)$ as rings.
  (d) Suppose that $e_1, e_2, \ldots, e_n$ are central idempotents of R, obeying $\sum e_j = 1$ and $e_i e_j = 0$ for $i \neq j$. Show that $R \cong \prod e_j R e_j$ as rings.

  A set of idempotents $\{e_1, e_2, \ldots, e_n\}$ as in part (16d) is called an ***orthogonal idempotent decomposition***.

  (e) Let $\pi_1, \pi_2, \ldots, \pi_k$ be central idempotents of R. Let $\{e_1, e_2, \ldots, e_{2^k}\}$ be the set of all products $q_1 q_2 \cdots q_k$ where each q_j is either π_j or $1 - \pi_j$. Show that $\{e_1, e_2, \ldots, e_{2^k}\}$ is an orthogonal idempotent decomposition.

(17) This problem displays standard applications of the Chinese Remainder Theorem over $\mathbb{Z}$.
  (a) Let n be a positive integer with prime factorization $n = \prod p_j^{e_j}$. Give a formula for the number of ordered pairs $(a, b) \in \{0, 1, 2, \ldots, n-1\}^2$ such that $\mathrm{GCD}(a, b, n) = 1$.
  (b) An integer n is called squarefree if it is not divisible by k^2 for any $k > 1$. Show that there is some integer N such that $N, N+1, \ldots, N+2019$ are all **not** squarefree.

(18) Let R be a commutative ring, let $a_1, a_2, \ldots, a_n$ be elements of R such that $(a_1, \ldots, a_n) = R$. Let M be a left R-module such that $a_i a_j M = 0$ for $i \neq j$. Show that

$$M = a_1 M \oplus a_2 M \oplus \cdots \oplus a_n M.$$

(19) Let R be the ring of integer quaternions: R is a free $\mathbb{Z}$-module with basis $1, i, j, k$, and multiplication $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$. Let p be an odd positive prime integer.
  (a) Show that there are integers u and v with $u^2 + v^2 + 1 \equiv 0 \bmod p$. (Hint: Pigeonhole principle.)
  (b) Show that there is a well-defined map of rings $R/pR \longrightarrow \mathrm{Mat}_{2\times 2}(\mathbb{Z}/p\mathbb{Z})$ with $i \mapsto \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $j \mapsto \left[\begin{smallmatrix} u & v \\ v & -u \end{smallmatrix}\right]$.
  (c) Show that the map in (19b) is an isomorphism. (Hint: If you haven't used that p is odd, your proof is broken.)
  (d) Show that R has a left ideal J with $|R/J| = p^2$.

[1] It is possible to remove this condition; this will appear on a future problem set.