Math 412 Homework 5

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Thursday, February 22nd, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. Consider the ring $M_2(\mathbb{R})$.

   (a) Take any nonzero 2×2 matrix A. Show that by multiplying A on the left by matrices of the form
   $$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
   we can do any elementary row operation to A.

   (b) State a way of interpreting column operations using matrix multiplication.

   (c) Prove that the only ideals in $M_2(\mathbb{R})$ are $\{0\}$ and $M_2(\mathbb{R})$.

(a) The first one is "add a times row one to row two," the second is "add a times row two to row one," the third is "multiply row one by c," the fourth is "multiply row two by c," and the last is "switch row one and row two."

(b) Multiplying on the right gives the same operations as above, but with "row" switched for "column."

(c) We need to show that if I is an ideal that contains a nonzero matrix A, then $I = M_2(\mathbb{R})$. From linear algebra, we know that we can use elementary row and column operations to transform A to the identity matrix. Thus, an ideal that contains A contains the identity matrix, and thus must be the whole ring!

2. Let $S_{\text{odd}} \subset \mathbb{Q}$ be the subset of rational numbers with odd denominators (when expressed in lowest terms).

   (a) Show that S_{odd} is a subring of $\mathbb{Q}$.

   (b) Let $I \subseteq S_{\text{odd}}$ be the subset of rational numbers with even numerator (when expressed in lowest terms). Prove that I is an ideal of S_{odd}.

   (c) Define a ring homomorphism $\phi\colon S_{\text{odd}} \to \mathbb{Z}_2$. What is the kernel?

(a) First, note that $1 = \frac{1}{1}, 0 = \frac{0}{1} \in S$. Given $\frac{a}{2b+1}, \frac{c}{2d+1} \in S$, where $a, b, c, d \in \mathbb{Z}$,
$$\frac{a}{2b+1} + \frac{b}{2c+d} = \frac{a(2d+1) + b(2b+1)}{(2b+1)(2d+1)} \text{ and } \frac{a}{2b+1}\frac{b}{2c+d} = \frac{ab}{(2b+1)(2d+1)}.$$
These fraction representations might not be expressed in the lowest possible terms, but since $2 \nmid 2b+1)(2d+1)$, their lowest possible terms will still have odd denominators.

We conclude that S is a subset of $\mathbb{Q}$ that is closed for addition and multiplication and contains 1 and 0. To check that S is a subring, all that remains to check is that S is closed for additive inverses. And indeed,

$$-\frac{a}{2b+1} = \frac{-a}{2b+1} \in S.$$

(b) Again, we start by noting that $0 = \frac{0}{1} \in I$. Given integers a, b, c, d,

$$\frac{2a}{2b+1} + \frac{2c}{2d+1} = \frac{2\left(a(2d+1) + b(2b+1)\right)}{(2b+1)(2d+1)} \in I.$$

Notice again that this might not be a representation in lowest possible terms, but that 2 divides the numerator and not the denominator, which implies that after reducing the fraction to its lowest possible terms, that will still hold. Similarly,

$$\frac{2a}{2b+1}\frac{2c}{2d+1} = \frac{4ac}{(2b+1)(2d+1)} \in I.$$

3. Let F be a field, and let $f \in \mathbb{F}[x]$. Two polynomials $g, h \in \mathbb{F}[x]$ are **congruent modulo** f if $f|(g-h)$. We write $g \equiv h \mod f$. The set of all polynomials congruent to g modulo f is written $[g]_f$. For this problem, we fix a polynomial $f \in \mathbb{F}[x]$ of degree $d > 0$.

   (a) Prove that every congruence class $[g]_f$ contains a *unique* polynomial in the set $S = \{h(x) \in F[x] \ : \ h(x) = 0 \text{ or } \deg h(x) < d\}$.

   (b) How many distinct congruence classes are there for $\mathbb{Z}_2[x]$ modulo $x^3 + x$?

   (c) How many distinct congruence classes are there for $\mathbb{Z}_3[x]$ modulo $x^2 + x$?

(a) For each congruence class modulo f, pick some element g in that congruence class. Let r be the remainder of dividing g by f; then r has degree less than d or $r = 0$, and $f|(g-r)$ by definition of r. So $r \in [g]_f$ and $r \in S$. That is, we have shown that every congruence class contains at least one element of S.

Let g and h be two polynomials in S which are both in the same congruence class modulo f. Since g and h are in the same congruence class, then $f|g-h$. Since g and h are both in S, $g-h$ is either 0 or a polynomial of degree less than d. Since f can't divide a non-zero polynomial of degree smaller than d, we get that $g - h = 0$. Hence, each congruence class contains at most one polynomial in S.

(b) Based on the previous part, we just need to count the number of polynomials in $\mathbb{Z}_2[x]$ that are 0 or have degree less than 3. That leaves 2 possibilities for the coefficients of x^2, x and the constant term respectively. Hence, the answer is $2^3 = 8$.

(c) Similarly, we just need to count the number of polynomials in $\mathbb{Z}_3[x]$ that are 0 or have degree less than 2. That leaves 3 possibilities for the coefficients of x and the constant term respectively. Hence, the answer is $3^2 = 9$

4. What are the subrings of $\mathbb{Q}$? We have $\mathbb{Z}$, $\mathbb{Q}$, and according to the previous problem, the subring S of rational numbers with odd denominators.

   (a) Prove that the subset
$$\mathbb{Z}[1/2] := \left\{ \frac{a}{2^m} \middle| a, m \in \mathbb{Z} \text{ and } m \geq 0 \right\} \subset \mathbb{Q}$$
   is a subring.

   (b) Let $R \subset \mathbb{Q}$ be a subring. Define:
$$\Pi(R) := \left\{ p \text{ a positive prime} \middle| \frac{1}{p} \in R \right\} \subset \mathcal{P} \text{ (the set of positive primes).}$$
   Compute $\Pi(\mathbb{Z})$, $\Pi(\mathbb{Q})$, $\Pi(\mathbb{Z}[1/2])$, $\Pi(S_{\text{odd}})$ (no proof needed).

   (c) (Tricky!) Given set of the positive prime numbers $\Gamma \subset \mathcal{P}$, define a subring denoted $\mathbb{Z}[1/\Gamma]$ such that $\Pi(\mathbb{Z}[1/\Gamma]) = \Gamma$.

   (d) (This is also hard!) Prove that two subrings $R_1, R_2 \subset \mathbb{Q}$ are equal $\iff$ $\Pi(R_1) = \Pi(R_2)$. Conclude, that the subrings of $\mathbb{Q}$ are in bijection with the subsets of the positive prime numbers!

(a) We have $1 = 1/2^0 \in \mathbb{Z}[1/2]$. For any two numbers in $\mathbb{Z}[1/2]$ of the form $a/2^m$ and $b/2^n$. Then
$$(a/2^m) + (b/2^n) = (a2^n + b2^m)/2^{m+n} \in \mathbb{Z}[1/2], \text{ and}$$
$$(a/2^m)(b/2^n) = (ab)/(2^{m+n}) \in \mathbb{Z}[1/2].$$
Finally $-a/2^m \in \mathbb{Z}[1/2]$. So $\mathbb{Z}[1/2]$ contains 1, is closed under $+/\times$ and inverses. Thus $\mathbb{Z}[1/2]$ is a subring.

(b) $\Pi(\mathbb{Z}) = \emptyset$, $\Pi(\mathbb{Q}) = \mathcal{P}$, $\Pi(\mathbb{Z}[1/2]) = \{2\}$, and $\Pi(S_{\text{odd}}) = \{3, 5, 7, 11, \dots\}$.

(c) Consider a subset $\Gamma \subset \mathcal{P}$. Define:
$$\mathbb{Z}[1/\Gamma] := \left\{ \frac{a}{b} \in \mathbb{Q} \middle| \begin{array}{l} \text{the positive prime factors of} \\ b \text{ are contained in } \Gamma \end{array} \right\}.$$
Then for two numbers $a_1/b_1, a_2/b_2 \in \mathbb{Z}[1/\Gamma]$ we have:
$$a_1/b_1 + a_2/b_2 = (a_1 b_2 + a_2 b_1)/(b_1 \cdot b_2) \in \mathbb{Z}[1/\Gamma].$$
Obvserve, that if the positive prime factors of b_1 and b_2 are in Γ then by the FTA, the same holds for $b_1 \cdot b_2$. The rest of the properties of subrings follow similarly. Finally, it is easy to see that $\Pi(\mathbb{Z}[1/\Gamma]) = \Gamma$!

(d) If two subrings are equal, then $1/p \in R_1 \iff 1/p \in R_2$. Thus $\Pi(R_1) = \Pi(R_2)$. In the other direction, if $\Pi(R_1) = \Gamma \subset \mathcal{P}$ then we want to show that $R_1 = \mathbb{Z}[1/\Gamma]$. Pick $a/b \in R_1$ in reduced form, and let p be any prime factor of b. Then we have $a/b = a/(p \cdot q)$. As R_1 is closed under addition this shows that
$$R_1 \ni a/p = (a/(p \cdot q) + \cdots + a/(p \cdot q)) \text{ (q times).}$$

We know $p \not| a$ as a/b was in reduced form. So by Bezout's identity we can write

$$1/p = (as + pt)/p = s \cdot (a/p) + t$$

for some integers s and t. Therefore, $1/p \in R$, so $p \in \Pi(R) = \Gamma$. But then every prime factor of b appears in Γ, so $a/b \in \mathbb{Z}[1/\Gamma]$ which proves $R_1 \subset \mathbb{Z}[1/\Gamma]$.

In the other direction. For $a/b \in \mathbb{Z}[1/\Gamma]$, assume b is positive and consider the prime factorization

$$b = p_1 \cdots p_m$$

then all the primes p_i are in Γ. Thus $1/p_i \in R_1$. So

$$1/b = (1/p_1) \cdots (1/p_m) \in R_1$$

and similarly,

$$R_1 \ni ((1/b) + \cdots + (1/b)) \text{ (a times)},$$

which proves $\mathbb{Z}[1/\Gamma] \subset R_1$ and proves the subring is unique.

Thus the subrings of $\mathbb{Q}$ are in bijection with the subsets of the positive prime numbers!