Homework #5

Problems to hand in on Thursday, February 21, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) Let $R = \mathbb{R}[x, y]$ be the polynomial ring in two variables x, y.

   a) Let $S \subseteq \mathbb{R}^2$. Show that the set

   $$I_S := \{f(x, y) \in R \mid f(a, b) = 0 \text{ for all } (a, b) \in S\}$$

   is an ideal of $\mathbb{R}[x, y]$.

   b) If $S = \{(0, 0)\}$, what is I_S?

   c) Show that, with I_S as in b), $R/I_S \cong \mathbb{R}$.

Solution.

(a) Let $f(x, y), g(x, y) \in I_S$. Then, $(f + g)(a, b) = f(a, b) + g(a, b) = 0$ for all $(a, b) \in S$, so $(f + g)(x, y) \in I_S$. Let $h(x, y) \in R$. Then $(fh)(a, b) = f(a, b)h(a, b) = 0$ for all $(a, b) \in S$, so $(fh)(a, b) \in R$. Finally, $0 \in I_S$, so I_S is an ideal.

(b) A function $f(x, y)$ is in I_S if and only if $f(0, 0) = 0$, which happens if and only if the constant term of f is zero.

(c) First, we note that $f(x, y)$ is equivalent to $g(x, y)$ modulo I_S if and only if the difference is in I_S, which happens if and only if they have the same constant term. Thus, there is a map from R/I_S to $\mathbb{R}$ sending $f(x, y) + I_S$ to $f(0, 0)$ (the constant term of f), and this function is well-defined, since another element in $f(x, y) + I_S$ must have the same constant term. This map is injective, since elements in different classes have different constant terms. It is surjective, since any real number is the constant term of some polynomial (e.g., a constant polynomial). Finally, the homomorphism properties hold: $(f + g)(0, 0) = f(0, 0) + g(0, 0)$, $(fg)(0, 0) = f(0, 0) + g(0, 0,$ and $f(0, 0) = 1$ for $f(x, y) = 1$.
Alternatively, we could use the first isomorphism theorem here.

2) 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 $M_2(\mathbb{R})$.

Solution.

(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!

3) Let $\mathbb{F}$ be a field, and $R = \mathbb{F}[x]$ be a polynomial ring. For $f(x) \in R$, we say that two polynomials $g(x), h(x)$ are **congruent modulo** $f(x)$ if $f(x)|(g(x) - h(x))$. We write $g(x) \equiv h(x) \bmod f(x)$ to denote this.[1]

a) Show that for $\lambda \in \mathbb{F}$, and any $a(x) \in R$, $a(x) \equiv a(\lambda) \bmod x - \lambda$.

b) Suppose that the greatest common divisor of $b(x)$ and $c(x)$ is 1. Show that for *any* $d(x)$, there is a polynomial $e(x)$ that solves the congruence equation $c(x)e(x) \equiv d(x) \bmod b(x)$.

c) Suppose again that the greatest common divisor of $f(x)$ and $g(x)$ is 1. Show that for *any* $h(x)$ and $i(x)$, there is a polynomial $j(x)$ that solves the system of congruence equations

$$\begin{cases} j(x) \equiv h(x) \bmod f(x) \\ j(x) \equiv i(x) \bmod g(x). \end{cases}$$

d) Let $\alpha, \beta, \gamma, \delta \in \mathbb{F}$, with $\alpha \neq \beta$. Use the previous parts to show that there is a polynomial $k(x) \in R$ such that $k(\alpha) = \gamma$ and $k(\beta) = \delta$.

Solution.

(a) This is essentially the Remainder Theorem from the text/worksheet: if we divide $a(x)$ by $x - \lambda$ the remainder is $a(\lambda)$; since $a(x)$ is congruent to its remainder, the statement is true.

(b) We know that there are polynomials $e'(x)$ and $e''(x)$ such that $b(x)e'(x)+c(x)e''(x) = 1$. Take $e(x) = d(x)e'(x)$.

(c) We know that there are polynomials $j'(x)$ and $j''(x)$ such that $j'(x)f(x)+j''(x)g(x) = 1$. Take $j(x) = j'(x)f(x)i(x) + j''(x)g(x)h(x)$.

(d) Since $(x - \alpha)$ and $(x - \beta)$ are coprime, by part (c), there is a polynomial such that $k(x) \equiv \gamma \bmod (x - \alpha)$ and $k(x) \equiv \delta \bmod (x - \beta)$. By part (a), this means that $k(\alpha) \equiv \gamma \bmod (x - \alpha)$ and $k(\beta) \equiv \delta \bmod (x - \beta)$. In both congruence equations, the two sides are constants, so they must be equal (each congruence class here contains at most one constant). Thus, this $k(x)$ works.

[1] This is a special case of congruence modulo an ideal; namely congruence modulo the ideal $(f(x))$.

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

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

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

   (c) Show that the quotient ring S/I is isomorphic to $\mathbb{Z}_2$.

Solution.

(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,

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

(c) We will show that S/I has two elements, and thus must be isomorphic to $\mathbb{Z}_2$. To do this, note that every element in S that is not in I is of the form $\frac{2a+1}{2b+1}$, where $a, b \in \mathbb{Z}$. We will show that every element of this form is congruent to 1 modulo I, which implies that there are only two classes modulo I. An indeed,

$$\frac{2a+1}{2b+1} - \frac{1}{1} = \frac{2a+1-(2b+1)}{2b+1} = \frac{2(a-b)}{2b+1} \in I.$$

To give an explicit isomorphism S/I to $\mathbb{Z}_2$, we send $0 + I$ to $[0]_2$ and $1 + I$ to $[1]_2$.