Math 341, Modules and Rings I – Fall 2020
Course website: `https://sites.aub.edu.lb/kmakdisi/`
Problem set 2, due Tuesday, September 29 at 2pm via Moodle

Exercises from Jacobson, BA I:
Section 3.1, exercise 4.
Section 3.2, exercises 2, 4, 5.

Additional Exercises (also required):

Exercise A2.1: Let $a, b, c, d, s, t \in \mathbf{Z}$, and define u, w by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} u \\ w \end{pmatrix}.$$

a) Show that one GCD is a factor of the other: $\gcd(s,t) \mid \gcd(u,w)$.

b) Show that if the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant ± 1, then in fact we have $\gcd(s,t) = \gcd(u,w)$.

c) Show more generally that $\gcd(u,w) \mid (\det M) \cdot \gcd(s,t)$.

Remark: this setup generalizes to $\gcd(s_1, \ldots, s_n)$, the GCD of n integers. M is replaced by an $n \times n$ matrix in $M_n(\mathbf{Z})$.

Exercise A2.2: Find $a \in \mathbf{Z}$ which simultaneously satisfies $a \equiv 3 \bmod 7$, $a \equiv 4 \bmod 11$, and $a \equiv 1 \bmod 13$.

Note: this is essentially an exercise in the Chinese Remainder Theorem, using the isomorphism $\mathbf{Z}/\langle 1001 \rangle \cong \mathbf{Z}/\langle 7 \rangle \times \mathbf{Z}/\langle 11 \rangle \times \mathbf{Z}/\langle 13 \rangle$.

Exercise A2.3: Take the field $F = \mathbf{Z}/\langle 5 \rangle = \{0,1,2,3,4\}$ (we really ought to write $\{\bar{0}, \bar{1}, \ldots\}$ but will usually not bother to do so), and consider the ring $R = F[x]$.

a) Using the extended Euclidean algorithm, find the (monic) GCD $d = d(x)$ of the following two polynomials in $F[x]$, and find polynomials $s(x), t(x)$ such that $d = sf + tg$:

$$f = x^6 + 3x^3 + 2, \qquad g = 2x^5 + x^3 + x^2 + 4x.$$

b) Factor each of f and g into irreducible factors, and use the factorization to give another way to find the GCD d.

Exercise A2.4: a) Find integers s, t such that $100s + 79t = 1$.

b) Let G be a cyclic group of order 100, written multiplicatively: so there is a generator g, and $G = \{1, g, g^2, \ldots, g^{99}\}$ with $g^{100} = 1$. Show that every element $h \in G$ can be written as $h = k^{79}$ for a unique $k \in G$.

Exercise A2.5: In this exercise, we view $\mathbf{Q}$ as a $\mathbf{Z}$-module. The two parts are basically unrelated.

a) Let $M = \langle 14/15, 12/25 \rangle$ be the submodule of $\mathbf{Q}$ generated by $14/15$ and $12/25$. Show that M is cyclic, i.e., there exists an element $x \in M$ with $M = \langle x \rangle$. Also find explicit $m, n \in \mathbf{Z}$ such that $x = m \cdot 14/15 + n \cdot 12/25$.

b) In the quotient module $\mathbf{Q}/\mathbf{Z}$, write the coset $a/b + \mathbf{Z}$ as $[a/b]$. (Here $a/b \in \mathbf{Q}$.) Consider the submodule $N = \langle [7/6], [7/10] \rangle$. Again show that N is cyclic: this time, show that $N = \langle [1/30] \rangle$, and find one choice of $m, n \in \mathbf{Z}$ such that $m[7/6] + n[7/10] = [1/30]$. (Bonus: can you describe **all** possible choices of m and n in a simple way?)

Exercise A2.6: For all of the following choices of $\mathbf{Z}$-modules M and N, describe: (i) all elements $f \in \mathrm{Hom}_{\mathbf{Z}}(M, N)$; (ii) For all f, the $\mathbf{Z}$-modules $\mathrm{Ker}\, f$, $\mathrm{Image}\, f$, and $\mathrm{Coker}\, f$. (Hint: they are all cyclic in this example, which is not typical — even for $\mathbf{Z}$-modules.)

a) $M = \mathbf{Z}$, $N = \mathbf{Z}$.
b) $M = \mathbf{Z}$, $N = \mathbf{Z}/\langle 6 \rangle$.
c) $M = \mathbf{Z}/\langle 6 \rangle$, $N = \mathbf{Z}$.
d) $M = \mathbf{Z}/\langle 15 \rangle$, $N = \mathbf{Z}/\langle 6 \rangle$.

Look at, but do not hand in:
BA I, 3.1.2. 3.1.5, 3.2.1, 3.2.7, 3.2.8.