Math 323 Homework 2

Problem 2 (Chapter 2.3)

Prove that if R is a commutative ring then $AB = 1$ in $M_n(R)$ implies $BA = 1$. (This is not always true for non-commutative R.)

Solution. Since $AB = 1$, we have

$$\begin{aligned}
AB &= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \\
&= \begin{pmatrix} \sum_i a_{1i}b_{i1} & \sum_i a_{1i}b_{i2} & \cdots & \sum_i a_{1i}b_{in} \\ \sum_i a_{2i}b_{i1} & \sum_i a_{2i}b_{i2} & \cdots & \sum_i a_{2i}b_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_i a_{ni}b_{i1} & \sum_i a_{ni}b_{i2} & \cdots & \sum_i a_{ni}b_{in} \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = 1
\end{aligned}$$

Hence, for all $1 \leq j, k \leq n$, we have $\sum_i a_{ji}b_{ik} = 0$ when $j \neq k$ and $\sum_i a_{ji}b_{ik} = 1$ when $j = k$. We can then compute

$$\begin{aligned}
BA &= \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \\
&= \begin{pmatrix} \sum_i b_{1i}a_{i1} & \sum_i b_{1i}a_{i2} & \cdots & \sum_i b_{1i}a_{in} \\ \sum_i b_{2i}a_{i1} & \sum_i b_{2i}a_{i2} & \cdots & \sum_i b_{2i}a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_i b_{ni}a_{i1} & \sum_i b_{ni}a_{i2} & \cdots & \sum_i b_{ni}a_{in} \end{pmatrix} \\
&= \begin{pmatrix} \sum_i a_{1i}b_{i1} & \sum_i a_{2i}b_{i1} & \cdots & \sum_i a_{ni}b_{i1} \\ \sum_i a_{1i}b_{i2} & \sum_i a_{2i}b_{i2} & \cdots & \sum_i a_{ni}b_{i2} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_i a_{1i}b_{in} & \sum_i a_{2i}b_{in} & \cdots & \sum_i a_{ni}b_{in} \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = 1
\end{aligned}$$

where the third line is done because R is commutative, and the fourth line is by our observation from before due to $AB = 1$.

Problem 5 (Chapter 2.4)

Verify that the set I of quaternions x in which all the coordinates α_i are either integers or all are halves of odd integers is a subring of $\mathbb{H}$. Is this a division sub-ring? Show that $T(x)$ and $N(x) \in \mathbb{Z}$ for any $x \in I$. Determine the group of units of I.

Solution. Recall $x \in \mathbb{H}$ is $x = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix} = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$. The product of x and $\begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$ is $\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ where $u = ac - b\bar{d}$, $v = ad + b\bar{c}$. From question 4 from section 2.1 (we did this last homework), by slightly changing the proof by swapping all the $\sqrt{-3}$ to $\sqrt{-1}$, but doing literally the same thing, we have that the set of complex numbers with components either integers or half of odd integers is a subring of $\mathbb{C}$, call it I', so u, v are both in I' as well, and both either have components that are integers or half of odd integers. So I is a subring of $\mathbb{H}$.

Let $x \in I$. Recall $T(x) = 2\alpha_0$. If α_0 is an integer, $2\alpha_0 \in \mathbb{Z}$, and if $\alpha_0 = \frac{l}{2}$ where l is odd, then $2\alpha_0 = l \in \mathbb{Z}$. Either way, $T(x) \in \mathbb{Z}$. Recall $N(x) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$. If $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$, then closure of multiplication and addition in $\mathbb{Z}$ implies that $N(x) \in Z$. If $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are all half of odd integers, then there exists odd integers l_0, l_1, l_2, l_3 such that $\alpha_i = l_i/2$. Then $N(x) = \frac{l_0^2}{4} + \frac{l_1^2}{4} + \frac{l_2^2}{4} + \frac{l_3^2}{4} = \frac{l_0^2+l_1^2+l_2^2+l_3^2}{4}$. Now, since l_0, l_1, l_2, l_3 are all odd, there exists integers m_0, m_1, m_2, m_3 such that $l_i = 2m_i + 1$. Then $l_i^2 = 4m_i^2 + 4m_i + 1$. Hence

$$N(x) = \frac{4m_0^2 + 4m_0 + 4m_1^2 + 4m_1 + 4m_2^2 + 4m_2 + 4m_3^2 + 4m_3 + 4}{4} = m_0^2 + m_0 + m_1^2 + m_1 + m_2^2 + m_2 + m_3^2 + m_3 + 1$$

and again, by the closure of multiplication and addition in $\mathbb{Z}$, since all $m_i \in \mathbb{Z}$, we have that $N(x) \in \mathbb{Z}$.

And then I will skip out on finding the units for this homework :)

Problem 2 (Chapter 2.5)

Show that the associative law holds for products of ideals: $(IJ)K = I(JK)$ if I, J, and K are ideals.

Solution. We prove set inclusion both ways. Let $a \in (IJ)K$. Then $a = \sum_n \left(\sum_m i_{n,m} j_{n,m}\right) k_n$, where $i_{n,m} \in I$, $j_{n,m} \in J$, and $k_n \in K$, since we can write ideal products as a sum of products. Then by distributivity and then associativity, we get $\sum_n \sum_m i_{n,m}(j_{n,m} k_n) \in I(JK)$. Hence, $(IJ)K \subseteq I(JK)$. And then the other direction is proved identically, with distributivity and associativity from the other side. Hence $I(JK) \subseteq (IJ)K$, so $I(JK) = (IJ)K$.

Problem 3 (Chapter 2.5)

Does the distributive law, $I(J + K) = IJ + IK$ hold?

Solution. We claim it does. We prove it by showing set inclusion in both directions. Let $a \in I(J + K)$. Then $a = \sum_n i_n(j_n + k_n)$. Then, by distributivity, $\sum_n i_n j_n + \sum_n i_n k_n \in IJ + IK$ by distributivity. So we have $I(J + K) \subseteq IJ + IK$. Now, it is clear that $J \subset J + K$ (just consider $k = 1$), so $IJ \subset I(J + K)$. Similarly, we have $IK \subset I(J + K)$. So, since $IJ + IK = IJ \cup IK$, we have that $IJ + IK \subseteq I(J + K)$. This shows that $I(J + K) = IJ + IK$.

Problem 4 (Chapter 2.6)

Let $A \in GL_2(\mathbb{Z}/(p))$ (that is, A is an invertible 2×2 matrix with entries in $\mathbb{Z}/(p)$). Show that $A^q = 1$ if $q = (p^2 - 1)(p^2 - p)$. Show also that $A^{q+2} = A^2$ for every $A \in M_2(\mathbb{Z}/(p))$.

Solution. We claim that if D is a finite division ring than $a^{|D|} = 1$ for every $a \in D$. This follows from group theory: D being a division ring means that $(D, \cdot)$ is a group, and for any finite group, $a^{|D|} = 1$. Now, consider the order of $GL_2(\mathbb{Z}/(p))$. In order for 2×2 matrix to be invertible, the columns need to be linearly independent. If we choose our leftmost column first, we can choose any permutation of two numbers in $\mathbb{Z}/(p)$ other than $0, 0$ (since this is linearly independent with nothing), so there are $p^2 - 1$ options (since there are p elements in $\mathbb{Z}/(p)$). Now, any vector that is linearly dependent to our first column $\vec{v}$ is of the form $a\vec{v}$ where $a \in \mathbb{Z}/(p)$, and so there are p choices of a, (and each $a\vec{v}$ is distinct, otherwise we form a subgroup of order less than p in $\mathbb{Z}/(p)$, but $|\mathbb{Z}/(p)|$, so this is impossible) hence, there are p columns linearly dependent on our first column. Hence there are $p^2 - p$ linearly independent ones. Hence, $|GL_2(\mathbb{Z}/(p))| = (p^2 - 1)(p^2 - p)$.

Now, by definition, $GL_2(\mathbb{Z}/(p))$ is a division ring (all the invertible matrices). So if $A \in GL_2(\mathbb{Z}/(p))$, we have $A^q = 1$ since $q = (p^2 - 1)(p^2 - p) = |GL_2(\mathbb{Z}/(p))|$.

It is clear then that $A^{q+2} = A^2$ when $A \in GL_2(\mathbb{Z}/(p))$, but I am too lazy to show his for $M_2(\mathbb{Z}/(p))$.

Problem 2 (Chapter 2.7)

Show that if u is a unit in R and η is a homomorphism of R into R' then $\eta(u)$ is a unit in R'. Suppose η is an epimorphism. Does this imply that η is an epimorphism of the group of units of R onto the group of units of R'?

Solution. If u is a unit in R, then there exists some $v \in R$ such that $uv = vu = 1_R$. Then $\eta(uv) = \eta(1_R) = 1_{R'}$ and $\eta(vu) = \eta(1_R) = 1_{R'}$. Since η is a homomorphism, we have $1_{R'} = \eta(uv) = \eta(u)\eta(v)$ and $1_{R'} = \eta(vu) = \eta(v)\eta(u)$. Hence, $\eta(u)$ is a unit in R', with inverse $\eta(v)$.

For the sake of contradiction, assume that there is a unit $u' \in R'$ such that $\eta^{-1}(u')$ is a set that does not contain a unit. Let v' be the inverse of u'. Then $1_{R'} = u'v' = \eta^{-1}(u')\eta^{-1}(v') = \eta^{-1}(u'v')$. So it works if $u'v'$ maps to 1... which I think is perfectly valid.

We claim that if $\eta\colon R \to R'$ is a homomorphism, it does NOT follow that η is an epimorphism of the group of units of R onto the group of units of R'. We provide the counter-example: $\eta\colon \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ by the natural map $x \mapsto \overline{x}$ where the equivalence relation is equivalence modulo 5. Clearly, this is a homomorphism, since $\eta(1) = \overline{1} = 1_{R'}$, $\eta(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \eta(x) + \eta(y)$ and $\eta(xy) = \overline{xy} = \bar{x}\bar{y} = \eta(x)\eta(y)$ (by elementary number theory). It is also clearly surjective, so η is an epimorphism. Now, the units in $\mathbb{Z}$ are 1 and -1, however, recall since 5 is prime, $(\mathbb{Z}/5\mathbb{Z}) \setminus \{\overline{0}\}$ is a group, i.e. $\mathbb{Z}/5\mathbb{Z}$ is a division ring and every element is invertible, so the units of $\mathbb{Z}/5\mathbb{Z}$ are $\overline{1}, \overline{2}, \overline{3}, \overline{4}$ (one can also just verify this by hand), and there is no surjective map from 2 to 4 elements, hence η cannot be surjective. So η from the units of $\mathbb{Z}$ is not surjective onto the units of $\mathbb{Z}/5\mathbb{Z}$.

Problem 4 (Chapter 2.7)

Show that if R is a commutative ring of prime characteristic p then $a \to a^p$ is an endomorphism of R (= homomorphism of R into R). Is this an automorphism?

Solution. Let our map be $\phi\colon R \to R$. Then $1 \mapsto 1^p = 1$. Also, if $a, b \in R$, $\phi(a+b) = (a+b)^p = a(a+b)^{p-1} + b(a+b)^{p-1} = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$ where we recover the binomial theorem because our ring is commutative (as discussed in class). Now, see that since p is prime, there are no values less than p (other than 1) that divides p. If we consider the prime factor decomposition of $k!$ where $0 \le k < p$, it contains no factors of p, hence $k! \nmid p!$. So, dividing $p!$ by two $k!$ and $(p-k)!$ still leaves a factor of p, so $p \mid \binom{p}{k}$ when $0 \le k < p$. Since R has characteristic p then, we have that $(a+b)^p = a^p + b^p$ (all of our terms go to 0). We also have $(ab)^p = \underbrace{ab\cdots ab}_{p \text{ times}} = a^p b^p = \phi(a)\phi(b)$ by the commutativity of R. Hence, ϕ is a homomorphism from R to itself, so it is a endomorphism.

Automorphism ff :(

Problem 9 (Chapter 2.7)

If $R_1, R_2, \ldots, R_n$ are rings we define the direct sum $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ *as for monoids and groups. The underlying set is $R = R_1 \times R_2 \times \cdots \times R_n$. Addition, multiplication, 0, and 1 are defined by*

$$\begin{aligned}(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)\\ (a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) &= (a_1b_1, a_2b_2, \ldots, a_nb_n)\\ 0 &= (0_1, 0_2, \ldots, 0_n)\\ 1 &= (1_1, 1_2, \ldots, 1_n)\end{aligned}$$

$0_i, 1_i$ the zero and unit of R_i. Verify that R is a ring. Show that the units of R are the elements $(u_1, u_2, \ldots, u_n)$, u_i a unit of R_i. Hence show that if $U = U(R)$ and $U_i = U(R_i)$ then $U = U_1 \times U_2 \times \cdots \times U_n$, the direct product of the U_i, and that $|U| = \prod |U_i|$ if the U_i are finite.

Solution. Closure under addition and multiplication follows directly from the definition, since $R_1, \ldots, R_n$ are each closed under the operations, and since $+$ and $\cdot$ are done component-wise, $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ satisfy closure for both addition and multiplication, and commutativity for addition. We can verify associativity: let $a_i, b_i, c_i \in R_i$, then

$$\begin{aligned}\big((a_1,\dots,a_n)+(b_1,\dots,b_n)\big)+(c_1,\dots,c_n) &= (a_1+b_1,\dots,a_n+b_n)+(c_1,\dots,c_n)\\ &= ((a_1+b_1)+c_1,\dots,(a_n+b_n)+c_n)\\ &= (a_1+(b_1+c_1),\dots,a_n+(b_n+c_n))\\ &= (a_1,\dots,a_n)+(b_1+c_1,\dots,b_n+c_n)\\ &= (a_1,\dots,a_n)+\big((b_1,\dots,b_n)+(c_1,\dots,c_n)\big)\end{aligned}$$

$$\begin{aligned}\big((a_1,\dots,a_n)(b_1,\dots,b_n)\big)(c_1,\dots,c_n) &= (a_1b_1,\dots,a_nb_n)(c_1,\dots,c_n)\\ &= ((a_1b_1)c_1,\dots,(a_nb_n)c_n)\\ &= (a_1(b_1c_1),\dots,a_n(b_nc_n))\\ &= (a_1,\dots,a_n)(b_1+c_1,\dots,b_n+c_n)\\ &= (a_1,\dots,a_n)\big((b_1,\dots,b_n)(c_1,\dots,c_n)\big)\end{aligned}$$

And commutativity

$$\begin{aligned}(a_1,\dots,a_n)+(b_1,\dots,b_n) &= (a_1+b_1,\dots,a_n+b_n)\\ &= (b_1+a_1,\dots,b_n+a_n)\\ &= (b_1,\dots,b_n)+(a_1,\dots,a_n)\end{aligned}$$

And distributivity

$$\begin{aligned}(a_1,\dots,a_n)\big((b_1,\dots,b_n)+(c_1,\dots,c_n)\big) &= (a_1,\dots,a_n)(b_1+c_1,\dots,b_n+c_n)\\ &= (a_1(b_1+c_1),\dots,a_n(b_n+c_n))\\ &= (a_1b_1+a_1c_1,\dots,a_nb_n+a_nc_n)\\ &= (a_1b_1,\dots,a_nb_n)+(a_1c_1,\dots,a_nc_n)\\ &= (a_1,\dots,a_n)(b_1,\dots,b_n)+(a_1,\dots,a_n)(c_1,\dots,c_n)\end{aligned}$$

$$\begin{aligned}\big((b_1,\dots,b_n)+(c_1,\dots,c_n)\big)(a_1,\dots,a_n) &= (b_1+c_1,\dots,b_n+c_n)(a_1,\dots,a_n)\\ &= ((b_1+c_1)a_1,\dots,(b_n+c_n)a_n)\\ &= (b_1a_1+c_1a_1,\dots,b_na_n+c_na_n)\\ &= (b_1a_1,\dots,b_na_1)+(c_1a_1,\dots,c_na_n)\\ &= (b_1,\dots,b_n)(a_1,\dots,a_n)+(c_1,\dots,c_n)(a_1,\dots,a_n)\end{aligned}$$

Where all of these follow from the associativity, additive commutativity, and distributivity of each of $R_1,\dots,R_n$.

Furthermore, if $a_i \in R_i$, then $0+(a_1,\dots,a_n) = (0_1+a_1,\dots,0_n+a_n) = (a_1,\dots,a_n)$ and similarly for $(a_1,\dots,a_n)+0$, and $1(a_1,\dots,a_n) = (1_1a_1,\dots,1_na_n) = (a_1,\dots,a_n)$ and similarly for $(a_1,\dots,a_n)1$, so our zero and unit are valid for $R_1 \oplus \dots \oplus R_n$.

Finally, we show that an additive inverse exists for all elements in $R_1 \oplus \dots \oplus R_n$. Consider $(a_1,\dots,a_n)$. Since in each R_i, there's some $-a_i$ such that $a_i+(-a_i) = (-a_i)+a_i = 0_i$, we have

$$(a_1,\dots,a_n)+(-a_1,\dots,-a_n) = (a_1-a_1,\dots,a_n-a_n) = (0_1,\dots,0_n) = 0$$

$$(-a_1,\dots,-a_n)+(a_1,\dots,a_n) = (-a_1+a_1,\dots,-a_n+a_n) = (0_1,\dots,0_n) = 0$$

hence, for any arbitrary element $(a_1,\dots,a_n) \in R_1 \oplus \dots \oplus R_n$, $(-a_1,\dots,-a_n)$ is an additive inverse.

To show that the units of R are the elements $(u_1,\dots,u_n)$, u_i is a unit of R_i, it is equivalent to show that $U = U_1 \times \dots \times U_n$ (where $U = U(R)$ and $U_i = U(R_i)$). We do this by set-inclusion in both directions. Assume $(a_1,\dots,a_n) \in U$. Then there is some $(b_1,\dots,b_n) \in R$ such that $(a_1,\dots,a_n)(b_1,\dots,b_n) = (b_1,\dots,b_n)(a_1,\dots,a_n) = 1$, So $(a_1b_1,\dots,a_nb_n) = (1_1,\dots,1_n)$ and $(b_1,a_1,\dots,b_na_n) = (1_1,\dots,1_n)$. Hence, $a_1b_1 = b_1a_1 = 1_1,\dots,a_nb_n =$

$b_n a_n = 1_n$. Hence, a_i has inverse b_i in R_i, so $a_i \in U_i$. Hence, $(a_1, \ldots, a_n) \in U_1 \times \cdots \times U)n$, so $U \subseteq U_1 \times \cdots \times U_n$. Now assume that $(u_1, \ldots, u_n) \in U_1 \times \cdots \times U_n$. Since u_i is a unit in R_i, there is some $v_i \in R_i$ such that $u_i v_i = v_i u_i = 1_i$. So consider $(v_1, \ldots, v_n) \in R$. Then $(u_1, \ldots, u_n)(v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_1 v_1) = (1_1, \ldots, 1_n) = 1$ and $(v_1, \ldots, v_n)(u_1, \ldots, u_n) = (v_1 u_1, \ldots, v_1 u_1) = (1_1, \ldots, 1_n) = 1$, hence $(u_1, \ldots, u_n) \in U$, so $U_1 \times \cdots \times U_n \subseteq U$. Therefore, $U = U_1 \times \cdots \times U_n$.

Finally, note that if $G = G_1 \times G_2 \times \cdots \times G_n$ and $|G_i| < \infty$ for all $1 \leq i \leq n$, we have $|G| = \prod_i |G_i|$. Hence, if all the U_i are finite, since $U = U_1 \times \cdots \times U_n$, we have $|U| = \prod_i |U_i|$.

Problem 10 (Chapter 2.7)

(Chinese remainder theorem). Let I_1 and I_2 be ideals of a ring R which are relatively prime *in the sense that $I_1 + I_2 = R$. Show that if a_1 and a_2 are elements of R then there exists an $a \in R$ such that $a \equiv a_i \pmod{I_i}$. More generally, show that if $I_1, \ldots, I_m$ are ideals such that $I_j + \bigcap_{k \neq j} I_k = R$ for $1 \leq j \leq m$, then for any $(a_1, a_2, \ldots, a_m)$, $a_i \in R$, there exists an $a \in R$ such that $a \equiv a_k \pmod{I_k}$ for all k.*

Solution. Recall $I_1 + I_2 := (I_1 \cup I_2)$. If $a_1 \in I_1$ and $a_2 \in I_2$, then $a = 0$ works. If $a_1 \in I_1$ but $a_2 \notin I_2$ (and so $a_2 \in I_1$ since $a_2 = i_1 + i_2$ and ff hmm now this seems a lot more trivial, we have $a = a_2$ works, since $a_1 - a_2 \in I_1$ since I is a subgroup with respect to addition, and $a_2 - a_2 = 0 \in I_2$ since I_2 must contain the zero since it is a group with respect to addition. The same works when $a_1 \notin I_1$ and $a_2 \in I_2$, i.e. $a = a_1$. ff