HW 13

7.3.13

The map $\varphi : \mathbb{C} \to M_2(\mathbb{R})$ given by $\varphi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ is an injective ring homomorphism. By proposition 5, this means $\mathbb{C}$ is isomorphic to the image of ϕ.

φ preserves addition: φ maps $a+bi+c+di$ to $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix}$, which is $\varphi((a+c)+(b+d)i)$.

φ preserves multiplication: φ maps $(a+bi)(c+di)$ to $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix}$, which is $\varphi(ac-bd+(ad+bc)i)$.

φ is injective: let $z = a+bi \in \ker\varphi$, then by comparing entries, $a=1, b=0$, hence $z=1$.

7.3.24a

We check that I is closed under addition: suppose $a, b \in \varphi^{-1}(J)$, then $\varphi(a) = a', \varphi(b') = b'$ for some $a', b' \in J$, hence $\varphi(a+b) = a'+b' \in J$, hence $a+b \in \varphi^{-1}(J)$.

We check that $\varphi^{-1}(J)$ is closed under left multiplication: suppose $a \in \varphi^{-1}(J), r \in R$, then $\varphi(a) = a' \in J$. We have $\varphi(ra) = \varphi(r)a' \in J$ since J is an ideal and $a' \in J$. Hence $ra \in \varphi^{-1}(J)$. The proof that I is closed under right multiplication is similar.

Applying it to the inclusion homomorphism φ, we have $\varphi^{-1}(S)$ is an ideal of R. $\varphi^{-1}(S)$ are all the elements in R that are mapped to an element in S, which means all the elements in R which are elements in S, which is exactly $R \cap S$.

7.3.24b

We check that $\varphi(J)$ is closed under addition. Let $a', b' \in \varphi(J)$, then there exists $a, b \in J$ such that $\varphi(a) = a', \varphi(b) = b'$. $a'+b' = \varphi(a+b) \in \varphi(J)$.

Supposing that φ is surjective, we check that $\varphi(J)$ is closed under left multiplication. Let $a' \in \varphi(J), r' \in R$, then there exists $a \in J$ such that $\varphi(a) = a'$. By surjectivity, there exists $r \in R$ such that $\varphi(r) = r'$, hence $r'a' = \varphi(ra) \in \varphi(J)$. The proof for right multiplication is similar.

Surjectivity is required. Otherwise, let $S = \mathbb{R}[x]$ and R be the subring of even polynomials (i.e. the ideal generated by x^2), and φ be the inclusion map. R is an ideal of R (since it is the whole ring) but the image is not an ideal since $x * x^2 \notin \varphi(R)$.

7.3.25

We can use a standard induction proof of the binomial theorem on n, like in this link `https://proofwiki.org/wiki/Binomial_Theorem`

In the induction step, the identity $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ is used. In R, this is interpreted as $1 + 1 \ldots = 1 + 1 \ldots$ where the LHS is $\binom{n}{k} + \binom{n}{k-1}$ copies of 1 and the RHS is $\binom{n+1}{k}$ copies. The equality follows from associativity of addition in R and the equality in $\mathbb{Z}$.

7.3.26a

Let f be the homomorphism. The proof that f preserves addition is the same proof that addition is associative in $\mathbb{Z}$ (e.g. by induction) since $f(a) + f(b) = (1 + 1 \ldots) + (1 + 1 \ldots) = f(a + b)$ where the dots denote repetition a total of a and b times respectively. f preserves multiplication because $f(a)f(b)$ is $(1 + 1 \ldots)(1 + 1 \ldots) = f(ab)$ which we can prove by induction on a and using the distributivity property of addition. Lastly $f(1) = 1$ by definition.

If $n = 0$, all the elements $1, 1 + 1, \ldots, 0, -1, -1 - 1, \ldots$ are distinct, as otherwise we have an equality which we could reduce to the form $1 + 1 + \ldots = 0$ for some finite sum on the left (e.g.: if two positive sums are equal, take their difference). Hence f is injective and has kernel $\{0\}$.

Otherwise, $n > 0$ and $f(n) = 0$. For $x \in \mathbb{Z}$ we can write $x = nq + r$ where $0 \leq r < n$ and some integer q. Then $f(x) = f(nq + r) = f(nq) + f(r) = f(r) \neq 0$. Hence $f(x) = 0 \iff n|x$.

7.3.26b

$\mathbb{Q}$ and $\mathbb{Z}[x]$ have characteristic 0 as they contain $\mathbb{Z}$ as a subring, and the inclusion map (which is injective) coincides with the map f.

$n\mathbb{Z}[x]$ is the ideal of multiples of n, which means it is the ideal of polynomials whose coefficients are multiples of n. We have $f(n) = 0$ since n and 0 are in the same coset of $n\mathbb{Z}[x]$ since $n \in n\mathbb{Z}[x]$. Hence the characteristic is at most n. Conversely, all the elements $f(0), f(1) \ldots f(n-1)$ are distinct, since otherwise if $f(a') = f(b'), a' > b'$ we could take the difference to get $f(a' - b') = 0$ but $a' - b' \notin n\mathbb{Z}[x]$ since $0 < a' - b' < n$ by construction. Hence the characteristic is n.

7.3.26c

For $0 < k < n, p|\binom{n}{k} = \frac{p!}{k!(p-k)!}$ as integers since p divides the numerator but none of the factors in the denominator, and by unique factorization in integers. Hence in R, we have $\binom{p}{k} = 0$. The result follows from the binomial theorem for $n = p$.

7.3.29

$N(R)$ is closed under left multiplication. Let $r \in R, x \in N(R)$ with $x^n = 0$. Then $(rx)^n = r^n x^n = r^n 0 = 0$ so $rx \in N(R)$. The proof for right multiplication follows because R is commutative.

$N(R)$ is closed under addition. Let $x, y \in N(R)$ with $x^n = y^m = 0$. We can replace the exponents with $N = \max(n, m)$ to get $x^N = y^N = 0$. Now $(x + y)^{2N} = \sum_{k=0}^{2N} \binom{2N}{k} x^k y^{2N-k} = 0$. For each term either $k \geq N$ or $2N - k \geq N$ as otherwise, their sum would be less than $2N$. Hence, each term is 0 and $x + y \in N(R)$.

7.3.30

Let $x \in R/N(R)$ be nilpotent with $x^n = 0$. We can write $x = r + N(R), x^n = r^n + N(R) = 0 + N(R)$. Hence $r^n \in N(R)$, that is there exists m such that $r^{nm} = 0 = r^{nm}$. Hence $r \in N(R)$ and we have $x = 0 + N(R)$, equivalently $x = 0$.

7.3.34a

$I + J$ contains I by taking $j = 0$ in the sum, and similarly it contains J. Let R contain both I and J. Let $i \in I, j \in J$. Then $i, j \in R$ and hence $i + j \in R$. Since i, j were arbitrary, $I + J \subseteq R$.

7.3.34b

Let $x \in IJ$; then $x = ij + i'j' + \ldots$ is a sum of products of i and j. Since I is a right ideal, $ij \in I, i'j' \in I$ and so on, hence $x \in I$. Similarly, since J is a left ideal, $x \in J$. Hence $x \in I \cap J$, hence $IJ \subseteq I \cap J$.

7.3.34c

We can take $R = Z, I = J = 2\mathbb{Z}$. Then $I \cap J = 2\mathbb{Z}$ but $IJ = 4\mathbb{Z}$ as an element of IJ is a sum of products of two even numbers, hence is divisible by 4.

7.3.34d

It suffices to show that $I \cap J \subseteq IJ$. Since $R = I + J$ is unital, we have $1 = i + j$ for some $i \in I, j \in J$.

Let $x \in I \cap J$. Then $x = 1x = ix + jx = ix + xj$. $ix \in IJ$ since $i \in I, x \in J$, and similarly $xj \in IJ$. Hence $x \in IJ$.

The hypothesis that R is unital is necessary. Otherwise with $I = J = R = 2\mathbb{Z}$ we have R is commutative and $I + J = R$ but $I \cap J = 2\mathbb{Z}, IJ = 4\mathbb{Z}$.

Also, $1 \in I + J$ does not imply $1 \in I \wedge 1 \in J$, as we can take $R = Z, I = 2\mathbb{Z}, J = 3\mathbb{Z}$.