Queen Mary University of London

MTH4104 Introduction to Algebra

Solutions to exam instance — Main exam period 2022

Question 1

(i) The elements of R are integers, while the elements of $\mathbb{Z}_m$ are congruence classes.

(ii) Informally: the rules for addition and multiplication in R and $\mathbb{Z}_m$ are "the same" apart from the difference between the way the elements are represented. That is, if $a \oplus b = c$ and $a \odot b = d$ in R, then $[a]_m + [b]_m = [c]_m$ and $[a]_m[b]_m = [d]_m$ in $\mathbb{Z}_m$.

(To use terminology not introduced in this module, R and $\mathbb{Z}_m$ are isomorphic.)

[A "what's the difference" question on this subject is unseen, but the answers are all very familiar bookwork facts.]

Question 2 Subtracting $[3]_{14}X + [1]_{14}$ from both sides gives

$$[5]_{14}X = [11]_{14}.$$

We can use the extended Euclidean algorithm to find $[5]_{14}$:

$$\begin{aligned} 4 &= 14 - 2 \cdot 5 \\ 1 &= 5 - 1 \cdot 4 \end{aligned}$$

so

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (14 - 2 \cdot 5) \\ &= -14 + 3 \cdot 5 \end{aligned}$$

implying $[5]_{14}^{-1} = [3]_{14}$. Multiply both sides of the equation by this inverse:

$$X = [3]_{14}[5]_{14}X = [3]_{14}[11]_{14} = [33]_{14} = [5]_{14}.$$

So the answer is $\boxed{x = 5}$.

[This is a standard exercise, which has appeared on tutorial sheets with different numbers.]

Question 3 Reading the proof of Theorem 1.7(b), we see that clause (a) in the definition of partition, stating $\emptyset \notin P$, is not used in the proof. So R will still be an equivalence relation. However, $\{[x]_R : x \in X\}$ need not equal P. For example, if $X = \{1\}$ and $P = \{\emptyset, \{1\}\}$, then $R = \{(1,1)\}$ and $\{[x]_R : x \in X\} = \{\{1\}\}$. So the answer is $\boxed{\text{d}}$.

[This kind of "what hypotheses are used in a proof, and what are the consequences" question is unseen.]

Question 4 $\boxed{\text{False}}$. This question is about leading zeroes in polynomials. One might think that q could start with $0x^2$ and thereby be equal to p, but in this case, the degree of q would actually be less than 2.

[A very similar question is in my formative quizzes.]

Question 5 $R = \boxed{\{a/2^n : a \in \mathbb{Z}, n \in \mathbb{N}\}}$ is a ring. The other choice $\{a/2 : a \in \mathbb{Z}\}$ is not a ring because it is not closed under multiplication: $1/2$ is an element but $1/2 \cdot 1/2 = 1/4$ is not.

Is R a ring with identity? $\boxed{\text{True}}$, $1 \in R$ is the identity element.

Is R a skewfield? $\boxed{\text{False}}$, $3 \in R$ has no inverse in R (in particular $1/3 \notin R$).

Is R a commutative ring? $\boxed{\text{True}}$, multiplication of real numbers is commutative.

[Other examples and nonexamples of subrings of $\mathbb{R}$ were gone over in lectures. These particular examples are unseen.]

Question 6

(i) The identity element is $e = \boxed{1/2}$. Proof (not required): we have

$$x ¤ \frac{1}{2} = 6x \cdot \frac{1}{2} - 2(x + \frac{1}{2}) + 1 = 3x - 2x - 1 + 1 = x$$

and also $1/2 ¤ x = x$ because ¤ is visibly commutative.

(ii) Given $x \in G$, let $y = (4x-1)/(12x-4)$. We have $y \in G$, because $y = \frac{1}{3} + (1/3)/(12x-4) > \frac{1}{3}$. Now

$$\begin{aligned}
x ¤ y &= x ¤ \frac{4x-1}{12x-4} \\
&= 6x\frac{4x-1}{12x-4} - 2\left(x + \frac{4x-1}{12x-4}\right) + 1 \\
&= (6x-2)\frac{4x-1}{12x-4} - 2x + 1 \\
&= \frac{4x-1}{2} - 2x + 1 \\
&= 2x - \frac{1}{2} - 2x + 1 \\
&= \frac{1}{2} = e.
\end{aligned}$$

Again, by commutativity, $y ¤ x = e$ as well. Thus y is the inverse of x, proving the inverse law.

[Proving group axioms is a standard exercise from lectures, tutorials, and coursework. This group operation is unseen.]

Question 7 This question uses standard algorithms from sections 6.2 and 6.3 of the notes which I will not rewrite here.

f in cycle notation is $\boxed{(3\ 5)(4\ 6)}$.

In two-line notation, $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \end{pmatrix}$ so $f^{-1}g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{pmatrix}$.
So one should type in $\boxed{3\ 5\ 4\ 1\ 2\ 6}$.
[This is a standard computation with many examples seen.]

Question 8 H must contain the inverse of x (by the inverse law), the identity element $e \in G$ (by the identity law: see the discussion in section 7.5 of the notes), and all powers of x (by repeated use of the closure law). H need not contain $x \diamond y$ for all $y \in G$: all elements of the group G can be written in this form, and proper subgroups exist.

By the above, any subgroup H of $\mathbb{Z}_{13}^{\times}$ containing $[9]_{13}$ must contain all its positive powers, the identity $[1]_{13}$, and its inverse $[9]_{13}^{-1} = [3]_{13}$: indeed, H must contain $[9]_{13}^{k}$ for all $k \in \mathbb{Z}$. Since $[9]_{13}^{3} = [1]_{13}$, the set of all powers is $\{[1]_{13}, [9]_{13}, [3]_{13}\}$. By e.g. writing out a Cayley table one can confirm that this set is closed under multiplication, so it is a subgroup, and is therefore the smallest subgroup sought. So the answer as typed in is $\boxed{\{1, 9, 3\}}$.
[The first part is more or less bookwork. The second part is unseen, but a similar question for fields instead of groups was on the tutorial sheets.]

Question 9 $\boxed{\text{False}}$, the product of two nonzero elements of R may be zero. An example is that $[2]_4[2]_4 = [0]_4$ in $\mathbb{Z}_4$.

The coefficient of x^4 in the product pq is $\boxed{ad}$.

No terms with x^k for $k > 4$ can appear in pq, so $\deg(pq)$ cannot exceed 4. By the first two parts of the question, the coefficient ad of x^4 may be zero, so the degree may be strictly less than 4. Indeed, in just the same way, all the products involved in all lower coefficients of pq may vanish as well, so pq may have any degree from 0 to 4, or have undefined degree, which is this module's convention for what happens when $pq = 0$.
[Examples of zero-divisors have been commented on. The second part is bookwork. The third part of the question is unseen but tutorial sheets have featured something similar.]

Question 10 [Note that this question has been replaced, and the replacement is in a separate PDF.] We must prove reflexivity, symmetry, and transitivity.
Reflexivity. Let $x \in \mathbb{C} \setminus \{0\}$. Then $x/x = 1 \in \mathbb{R}$, so $(x,x) \in S$. Therefore S is reflexive.
Symmetry. Let $x, y \in \mathbb{C} \setminus \{0\}$, and assume $(x,y) \in S$, that is, $y/x \in \mathbb{R}$. Also $y/x \neq 0$ because $y \neq 0$. Since $x/y = 1/(y/x)$ and the reciprocal of a nonzero real number is real, we have $x/y \in \mathbb{R}$. Therefore $(y,x) \in S$, so S is symmetric.
Transitivity. Let $x, y, z \in \mathbb{C} \setminus \{0\}$, and assume (x,y) and (y,z) are in S, that is, $y/x, z/y \in \mathbb{R}$. Since $z/x = (z/y) \cdot (y/x)$ and $\mathbb{R}$ is closed under multiplication, we have $z/x \in \mathbb{R}$. Therefore $(x,z) \in S$, so S is transitive.
[A standard kind of proof. Lectures have featured examples of such proofs for similar relations.]

Question 11 $\boxed{\{\{1,2\},\{3,4\},\{5,6\}\}}$ is a partition of X. The point of this question, of course, is just distinguishing different kinds of brackets.
[This is a notational point I emphasised in lecture and in my formative quizzes.]