# MODEL ANSWERS TO THE FIFTH HOMEWORK

§18: 12. This is a ring; it is a subring of the real numbers. It is commutative, with unity. It is (somewhat suprisingly) a field. Note that

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

Also note that if $a^2 - 2b^2 = 0$ then $a = b = 0$ as $\sqrt{2}$ is irrational. Thus if $a + b\sqrt{2} \neq 0$ then

$$\frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

is the multiplicative inverse of $a + b\sqrt{2}$.
16. The elements of $\mathbb{Z}_5$ are 0, 1, 2, 3 and 4. 0 is certainly not a unit.

$$1 \cdot 1 = 1 \qquad 2 \cdot 3 = 1 \qquad \text{and} \qquad 4^2 = 4 \cdot 4 = 1$$

so that the units are 1, 2, 3 and 4.
18. Suppose that $(a, b, c) \in \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$. Then $(a, b, c)$ is a unit if and only if we can find $(a', b', c')$ such that

$$(1, 1, 1) = (a, b, c) \cdot (a', b', c') = (aa', bb', cc').$$

But then $a$, $b$ and $c$ are units, so that $a = \pm 1$, $b \neq 0$ and $c = \pm 1$.
33. T: (a), (e), (g), (h), (i), (j)
F: (b), (c), (d), (f).
40. Suppose not, suppose that

$$\phi \colon 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$$

is an isomorphism. Let $a = \phi(2)$. Then

$$\begin{aligned} \phi(4) &= \phi(2 + 2) \\ &= \phi(2) + \phi(2) \\ &= a + a \\ &= 2a. \end{aligned}$$

On the other hand,

$$\begin{aligned} \phi(4) &= \phi(2 \cdot 2) \\ &= \phi(2) \cdot \phi(2) \\ &= a \cdot a \\ &= a^2. \end{aligned}$$

Thus $a^2 = 2a$. This equation holds in $3\mathbb{Z} \subset \mathbb{C}$. Thus $a$ is a complex solution of the polynomial equation:

$$x^2 = 2x.$$

We know the solutions to this equation, either $x = 0$ or $x = 2$. $2 \notin 3\mathbb{Z}$. Thus $x = 0$. In this case the kernel of $\phi$ is non-trivial and $\phi$ is not one to one. Thus $\phi$ is not an isomorphism.

46. By assumption we may find $m$ and $n$ such that $a^m = b^n = 0$. Let $d = m + n - 1$ and consider $(a + b)^d$. Note that

$$a^i = a^m a^{i-m} = 0 \qquad \text{and} \qquad b^j = b^n b^{j-n} = 0 \qquad \text{for } i \geq m \text{ and } j \geq n.$$

Therefore, if we apply the binomial theorem, which holds in a commutative ring by the usual inductive argument, we get

$$\begin{aligned}(a+b)^d &= \sum_{i+j=d} \binom{d}{i} a^i b^j \\ &= \sum_{i=m}^{d} \binom{d}{i} a^i b^{d-i} + \sum_{j=n}^{d} \binom{d}{j} a^{d-j} b^j \\ &= 0.\end{aligned}$$

§19: 1. We can factor this polynomial as follows:

$$x^3 - 2x^2 - 3x = x(x^2 - 2x - 3) = x(x-3)(x+1).$$

Thus three obvious solutions to the equation

$$x^3 - 2x^2 - 3x = x(x-3)(x+1) = 0$$

are $x = 0$, $x = 3$ and $x = -1 = 11$. However $\mathbb{Z}_{12}$ has zero divisors,

$$2 \cdot 6 = 3 \cdot 4 = 3 \cdot 8 = 4 \cdot 6 = 4 \cdot 9 = 6 \cdot 6 = 6 \cdot 8 = 6 \cdot 10 = 8 \cdot 9 = 0,$$

in $\mathbb{Z}_{12}$. The jumps between the numbers $x - 3$, $x$ and $x + 1$ are 1, 3 and 4.

So we also get the solutions $x = 5$, $x = 8$ and $x = 9$.

6. The identity in $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$.

$$n \cdot (1, 1) = (n, n).$$

This is equal to zero if and only if $n = 0$. Thus the characteristic is zero.

11.

$$\begin{aligned}(a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\ &= a^4 + 2a^2b^2 + b^4,\end{aligned}$$

using the binomial theorem and the fact that $4 = 0$ in the ring.

17. T: (b), (e), (f), (h), (i)

F: (a), (c), (d), (g), (j).

3. **Challenge Problems**

§18: 52. Suppose that $m$ and $n \in \mathbb{Z}$. Then we get $(m, n) \in \mathbb{Z}_r \times \mathbb{Z}_s$. Since there is an isomorphism

$$\phi\colon \mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$$

we may find $a \in \mathbb{Z}_{rs}$ such that $\phi(a) = (m, n)$. But then there is an integer $x$ which represents $a$ such that $x = m \mod r$ and $x = n \mod s$.

53. (a) Let $r_1, r_2, \dots, r_n$ be $n$ positive integers which are pairwise coprime, so that if $i \neq j$ then $r_i$ and $r_j$ are coprime. Let $r$ be the product of $r_1, r_2, \dots, r_n$. Then there is a ring isomorphism

$$\phi\colon \mathbb{Z}_r \longrightarrow \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_n}$$

Since $r_1, r_2, \dots, r_n$ are pairwise coprime, it follows that

$$\mathbb{Z}_r \qquad \text{and} \qquad \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_n}$$

are both cyclic groups of order $r$, with generators 1 and $(1, 1, \dots, 1)$. Therefore the map which sends $m$ to $m \cdot (1, 1, \dots, 1)$ is a group isomorphism. This map is also a ring isomorphism as

$$\begin{aligned}
\phi(ab) &= (ab) \cdot (1, 1, \dots 1) \\
&= [a \cdot (1, 1, \dots 1)][b \cdot (1, 1, \dots 1)] \\
&= \phi(a)\phi(b).
\end{aligned}$$

(b) The integers $a_1, a_2, \dots, a_n$ define an element $(a_1, a_2, \dots, a_n) \in \mathbb{Z}_{b_1} \times \mathbb{Z}_{b_2} \times \cdots \times \mathbb{Z}_{b_n}$. By part (a) we may find $a$ such that $\phi(a) = (a_1, a_2, \dots, a_n)$. $a$ corresponds to a positive integer $x$ such that $x = a_i \mod b_i$.