Algebra Sample Test

These answers have been transcribed from the barely legible handwriting that was given on Canvas. There thus may be errors in the solutions; please check and let me know if something's not quite right.

1. (a) (5 points) Compute the order of each element in $U(18)$.

Solution: $U(18) = \{1, 5, 7, 11, 13, 17\}$.

$5, 5^2, 5^3 = 5, 7, 17 \Rightarrow |5| > 3$.

The order of 5 should divide $|U(18)| = 6 \Rightarrow |5| = 6$.

$7, 7^2, 7^3 = 7, 13, 1 \Rightarrow |7| = 3$. Alternatively, $7 = 5^2, |5| = 6 \Rightarrow |7| = 3$.

$11, 11^2, 11^3 = 11, 13, 17 \Rightarrow |11| = 6$.

$13 = 11^2 \Rightarrow |13| = \frac{|11|}{2} = 3$. Or $13, 13^2, 13^3 = 13, 7, 1 \Rightarrow |13| = 3$.

$17 = 11^3 \Rightarrow |17| = \frac{6}{3} = 2$. Or $17, 17^2 = 17, 1 \Rightarrow |17| = 2$.

(b) (4 points) Prove that $U(18)$ is isomorphic to $U(14)$.

Solution:

Proof. From (a) it follows that $U(18)$ is cyclic, so $U(18) \approx \mathbb{Z}_6$.

It suffices to find an element of order 6 in $U(14)$:

$U(14) = \{1, 3, 5, 9, 11, 13\}$

$3^2 = 9, 3^3 = 13 \Rightarrow |3| > 3 \Rightarrow |3| = 6$

Thus $U(14)$ is cyclic, so $U(14) \approx \mathbb{Z}_6$. It follows that $U(18) \approx U(14)$. □

Or:

Proof. $U(14) = U(2 \cdot 7) = U(2) \oplus U(7)$, because $\gcd(2, 7) = 1$.

$U(2) = \{1\}$, $U(7) \approx \mathbb{Z}_6$, because 7 is prime.

It follows that $U(2) \oplus U(7) \approx \mathbb{Z}_6$, and thus $U(18) \approx U(14)$. □

2. (a) (4 points) Prove that the ring R defined by

$$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

is an integral domain.

Solution: $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ has no zero divisors:

$$
\begin{aligned}
0 &= (a+b\sqrt{2})(c+d\sqrt{2}) \\
\Rightarrow 0 &= (a-b\sqrt{2})(a+b\sqrt{2})(c+d\sqrt{2})(c-d\sqrt{2}) \\
\Rightarrow 0 &= (a^2-2b^2)(c^2-2d^2)
\end{aligned}
$$

Since $\mathbb{Z}$ has no zero divisors, it follows that $a^2-2b^2=0$ or $c^2-2d^2=0$.

$a^2-2b^3=0 \Rightarrow a^2=2b^2 \Rightarrow \left(\frac{a}{b}\right)^2=2$.

This is impossible, because $\sqrt{2}\notin\mathbb{Q}$.

It follows that R has no zero divisors and therefore it is an integral domain.

(b) (3 points) Is the ring S defined by

$$S=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$$

an integral domain?

Solution:

Proof. Just like in (a) we conclude that $(a+b\sqrt{2})(c+d\sqrt{2})=0$ implies that $a^2-2b^2=0$ or $c^2-2d^2=0, a,b,c,d\in\mathbb{Q}$.

$a^2-2b^2=0\Rightarrow\left(\frac{a}{b}\right)^2=0, \frac{a}{b}\in\mathbb{Q}$, contradiction.

Conclusion: S is an integral domain. □

(c) (2 points) Is the ring T defined by

$$T=\{a+b\sqrt{2}\mid a,b\in\mathbb{R}\}$$

an integral domain?

Solution:

Proof. $T=\mathbb{R}\Rightarrow$ field $\Rightarrow$ integral domain □

3. We want to paint the edges of a square made of iron wire using red and blue. We want to use Burnside's theorem to determine the number of different colorings.

(a) (3 points) What, in the terminology of Burnside's theorem, is the set S? What is the group of permutations S acting on S?

Solution: S is the set of all possible colorings, disregarding symmetries:

$$
S=\left\{\begin{array}{lllll}
rrrr, & brrr, & rbrr, & rrbr, & \\
rrbb, & rbrb, & rbbr, & bbrr, & brbr, \quad brrb, \\
rbbb, & brbb, & bbrb, & bbbr, & bbbb,
\end{array}\right\}\rightarrow |S|=16
$$

$G=D_4$, $|G|=8$.

(b) (4 points) Determine the number of orbits in S under G.

Solution: $D_4 = \{R_0, R_90, R_180, R_270, D, D', H, V$.

$$
\begin{aligned}
|\mathsf{fix}(R_0)| &= |S| = 16 \\
|\mathsf{fix}(R_90)| &= |\{rrrr, bbbb\}| = 2 \\
|\mathsf{fix}(R_180)| &= |\{rbrb, brbr, rrrr, bbbb\}| = 4 \\
|\mathsf{fix}(R_270)| &= |\mathsf{fix}(R_90)| = 2 \\
|\mathsf{fix}(H)| &= \left| \left\{ \begin{array}{cccc} rrrr, & rrrb, & rbrr, & rbrb, \\ bbbb, & bbbr, & rrbb, & brbr \end{array} \right\} \right| = 8 \\
|\mathsf{fix}(V)| &= |\mathsf{fix}(H)| = 8 \\
|\mathsf{fix}(D)| &= |\{rrrr, rbbr, brrb, bbbb\}| = 4 \\
|\mathsf{fix}(D')| &= |\mathsf{fix}(D')| = 4
\end{aligned}
$$

According to Burnside's theorem:

$$
\begin{aligned}
\#_{\mathsf{orbits}} &= \frac{1}{|G|} \sum_{\gamma \in G} |\mathsf{fix}(\gamma)| \\
&= \frac{1}{8}(16 + 2 + 4 + 2 + 8 + 8 + 4 + 4) = \frac{1}{8} \cdot 48 = 6
\end{aligned}
$$

(c) (4 points) Determine for each element in S the corresponding orbit.

Solution:

$$
\begin{aligned}
\mathsf{orb}_G(rrrr) &= \{rrrr\} \\
\mathsf{orb}_G(bbbb) &= \{bbbb\} \\
\mathsf{orb}_G(brrr) &= \{brrr, rbrr, rrbr, rrrb\} \\
\mathsf{orb}_G(rrbb) &= \{brrb, bbrr, rbbr, rrbb\} \\
\mathsf{orb}_G(rbrb) &= \{rbrb, brbr\} \\
\mathsf{orb}_G(rbbb) &= \{rbbb, brbb, bbrb, bbbr\}
\end{aligned}
$$

Check: 6 orbits with a total number of 16 elements.

4. Consider $p(x) \in \mathbb{Z}_3[x]$ defined by $p(x) = x^2 + 1$ and let $\mathbb{F}$ be defined as

$$\mathbb{F} = \mathbb{Z}_3[x] / < p(x) >$$

(a) (3 points) Argue that $\mathbb{F}$ is a field.

Solution: $p(0) = 1, p(1) = 2, p(2) = 2 \Rightarrow p(x)$ has no roots in $\mathbb{Z}_3$, $\deg_p(x) = 2 \Rightarrow p(x)$ is irreducible.

It follows that $< p(x) > is a maximal ideal in \mathbb{Z}_3[x] \Rightarrow \mathbb{Z}_3[x]/ < p(x) >$ is a field.

(b) (3 points) Describe the elements of $\mathbb{F}$.

Solution: Elements of $\mathbb{F}$ are of the form $a_0 + a_1 x + < p(x) >, a_0, a_1 \in \mathbb{Z}_3$.

(c) (2 points) How many elements does $\mathbb{F}$ have?

Solution: Using our solution to part b, it follows that $|\mathbb{F}| = 9$.

(d) (3 points) Prove that the multiplicative group $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is cyclic.

Solution:

Proof. $\mathbb{F}^*$ has 8 elements. Therefore, it suffices to find an element in $\mathbb{F}^*$ of which the order is greater than 4.

$$
\begin{aligned}
\text{Try } \alpha &= 1 + x + < p(x) > \\
\alpha^2 &= 1 + 2x + x^2 + < p(x) > \\
&= 1 + 2x + 2 + < p(x) > = 2x + < p(x) > \\
\alpha^3 &= (1 + x)2x + < p(x) > = 2x + 2x^2 + < p(x) > \\
&= 1 + 2x + < p(x) > \\
\alpha^4 &= (2x)^2 + < p(x) > = x^2 + < p(x) > \\
&= 2 + < p(x) > \\
&\Rightarrow |\alpha| > 4 \Rightarrow |\alpha| = 8 \\
&\Rightarrow \mathbb{F}^* \text{ is cyclic.}
\end{aligned}
$$

□

Question:	1	2	3	4	Total
Points:	9	9	11	11	40
Score:					