Math 320 - Spring 2019
Instructor: Christopher O'Neill
Practice Final Exam

Last Name: $\qquad$ First Name:

There are 7 questions, although each has a varying number of parts. This practice exam is longer than the actual final exam (in fact, this one is worth over 100 points!), so as to give extra practice. You will have two hours to take the actual final exam.
(1) Fill in the blanks in each of the following statements. No justification is required. (3 points each) (a) The prime factorization of 36 is $\qquad$ .
(b) For any $a \in \mathbb{Z}$, the only possible values of $\operatorname{gcd}(a, a+5)$ are $\qquad$ and $\qquad$ .
(c) The element $[8]_{12} \in \mathbb{Z}_{12}$ is a zero-divisor since multiplying by $\qquad$ yields $[0]_{12}$.
(d) Given $a=\left([2]_{3}, 0.5\right), b=\left([1]_{3}, 6\right) \in \mathbb{Z}_{3} \times \mathbb{R}$, we have $a+b=$ $\qquad$ and $a b=$ $\qquad$ .
(e) We have $45 \cdot 2345678=1055 \quad 5510$ (only one digit is missing).

Hint: don't do heavy arithmetic, use divisibility by 9 instead!
(f) The number of distinct roots of the polynomial $x^{3}+2 x+1$ over $\mathbb{Z}_{5}$ is $\qquad$ .
(g) Dividing $f(x)=x^{3}+2 x+1$ by $g(x)=x^{2}+x$ over $\mathbb{Q}$ yields $q(x)=$ $\qquad$ and $r(x)=$ $\qquad$ .
(h) Dividing $f(x)=x^{3}+2 x+1$ by $g(x)=x^{2}+x$ over $\mathbb{Z}_{7}$ yields remainder $r(x)=$ $\qquad$ .
(i) The smallest positive integer $m$ such that $\left[x^{m}\right]=[1]$ in $\mathbb{Z}_{2}[x] /\left\langle x^{2}+x+1\right\rangle$ is $\qquad$ $-$
(j) The number of elements in the quotient ring $\mathbb{Z}_{5}[x] /\left\langle x^{3}+x^{2}+1\right\rangle$ is $\qquad$ .
(k) The number of elements in the dihedral group $D_{9}$ is $\left|D_{9}\right|=$ $\qquad$ -
(l) Find the product of the permutations $\sigma$ and $\tau$ below.

$$
\sigma=\left(\begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
2 & 5 & 3 & 1 & 4
\end{array}\right) \quad \tau=\left(\begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
5 & 4 & 3 & 2 & 1
\end{array}\right) \quad \sigma \tau=\left(\begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
& & & & \\
\hline
\end{array}\right.
$$

(2) Each of the following sets $R$ with the given operations $\oplus$ and $\odot$ does not form a ring. For each, locate a ring axiom that is violated, and demonstrate that it is violated. (5 points each)
(a) The set $R$ of nonzero integers, with $a \oplus b=a b$ and $a \odot b=a b$ for all $a, b \in R$.
(b) The set $R$ of continuous functions on $\mathbb{R}$, with $f(x) \oplus g(x)=f(x) g(x)$ and $f(x) \odot g(x)=f(g(x))$ for all $f(x), g(x) \in R$.
(3) Each of the following maps is not an isomorphism of rings. For each, give an example demonstrating that one of the requirements is violated. (5 points each)
(a) The map $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{12}$ given by $a \mapsto[a]_{12}$.
(b) The map $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $a \mapsto a+1$.
(4) Factor $x^{5}+2 x^{4}+2 x^{3}+2 x+2 \in \mathbb{Z}_{3}[x]$ as a product of irreducibles. (10 points)
(5) Find $\operatorname{gcd}\left(x^{4}+2 x^{2}+x-1, x^{3}+x+1\right)$ over $\mathbb{Z}_{3}$. (10 points)
(6) Let $R=\mathbb{Z}_{5}[x] /\left\langle x^{2}+4\right\rangle$ and let $r=[x+1] \in R$. Locate 2 distinct equivalence classes $t, t^{\prime} \in R$, both nonzero, such that $r t=[0]$ and $r t^{\prime}=[0]$. (10 points)
(7) Determine whether each of the following statements is true or false. Briefly justify each answer, or provide a counterexample (if appropriate). (5 points each)
(a) The elements $\left[x^{2}+1\right]$ and $\left[x^{3}+1\right]$ in $\mathbb{Z}_{2}[x] /\left\langle x^{4}+x^{3}+1\right\rangle$ are multiplicative inverses.
(b) The ring $\mathbb{Z}_{3}[x] /\left\langle x^{3}+x+1\right\rangle$ is a field.
(c) We can conclude $x^{4}+x^{2}+4$ is irreducible in $\mathbb{Z}_{5}[x]$ since it has no roots in $\mathbb{Z}_{5}$.
(d) The set

$$
R=\left\{\left(\begin{array}{ll}
a & a \\
0 & a
\end{array}\right): a \in \mathbb{R}\right\} \subset M(\mathbb{R})
$$

is a subring of $M(\mathbb{R})$.
(e) For any $a, b \in \mathbb{Z}$, we have $\operatorname{gcd}(2 a+b, a+b)=\operatorname{gcd}(a, b)$.
(f) $(\mathbb{Z},+)$ is a group.
$(\mathrm{g})(\mathbb{Z}, \cdot)$ is a group.

