Math 113 Midterm April 23, 2019

Answer the questions in the spaces provided on the question sheets. If you run out of room for an answer, continue on the back of the page.
Unless stated otherwise, you may use a result without proving it if it was shown in one of the lectures, homeworks or readings.

Name: Dmitry

1. (20 points)

(a) (10 points) If R is a commutative ring and $a \in R$ is a zero divisor, prove that $b \cdot a$ is a zero-divisor for any $b \in R$.

given : $a \in R$ is zero-divisor
$\Rightarrow \exists 0 \neq a'$ with $a\,a' = 0$
$\Rightarrow$ $b \cdot a \cdot a' = 0$, for the same $a' \neq 0 \in R$.
$\Rightarrow$ $b \cdot a$ is a zero-divisor.

(b) (10 points) Do all zero-divisors in a commutative ring form a subring? Prove this or give a counterexample.

No. Consider $R = \mathbb{Z}_6$. 2, 3 are zero-divisors but $2+3=5$ is not, so not a subring.
Alternatively: consider $R = \mathbb{Z} \times \mathbb{Z}$. The $(1,0)$ and $(0,1)$ are zero-divisors, but $(1,1)$ is not.

2. (20 points) Find all solutions in $\mathbb{Z}_{35}$ to $x^2 + 31 = 0$.

$x^2+31 \equiv x^2-4 \equiv (x+2)(x-2)$.

In $\mathbb{Z}_5$, solutions $\pm 2 = \{2, 3\}$
(no more, since $\mathbb{Z}_5$ is a domain).
In $\mathbb{Z}_7$, solutions $\pm 2 = \{2, 5\}$.

So four solutions, $(\pm 2, \pm 2) \in \mathbb{Z}_5 \times \mathbb{Z}_7$.

Under iso $\varphi: \mathbb{Z}_{35} \simeq \mathbb{Z}_5 \times \mathbb{Z}_7$:

$\varphi(2) = (2,2) \Rightarrow 2$ is a solution
$\varphi(-2) = (-2,-2) \Rightarrow -2 \equiv 33$ is a solution
$\varphi(12) = (2,5) \equiv (2,-2) \Rightarrow 12$ is a solution
$\varphi(-12) = (-2,2) \Rightarrow -12 \equiv 23$ is a solution.

So there are four solutions:

$\{2, 33, 12, 23\}$.

3. (20 points)

(a) (5 points) Let $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Do a calculation to show that the residue of x^5 modulo $x^4 + x^3 + x^2 + x + 1$ is 1.

$$\begin{array}{r|l} x^5 & f(x) \\ \hline -xf(x) & x-1 \\ \hline -x^4-x^3-x^2-x & \\ +f(x) & \\ \hline 1 & \end{array}$$

(b) (5 points) Show that for $n \in \mathbb{N}$, we have $x^n \equiv 1 \mod f$ if and only if $n \equiv 0 \mod 5$.

($\Leftarrow$): If $n \equiv 0 \mod 5$ then $n = 5k$ for $k \in \mathbb{N}$.

$x^n = x^{5k} = (x^5)^k \equiv_f 1^k = 1$, so $x^n \equiv 1 \mod f$.

($\Rightarrow$) Given $x^n \equiv_f 1$. By previous part, $x^n = x^{5k} \cdot x^{n \bmod 5} \equiv_f x^{n \bmod 5}$ (some $k \in \mathbb{N}$). $n \bmod 5$ can be $0, 1, 2, 3, 4$. x^1, x^2, x^3 are remainders, so $\not\equiv 1$. $x^4 \equiv -x^3 - x^2 - x - 1$, so $\not\equiv 1$. Only remaining option is $n \equiv 0 \mod 5$.

(c) (5 points) Find the residue of x^{34} modulo $x^4 + x^3 + x^2 + x + 1$.

$x^{34} \equiv x^4 \equiv -x^3 - x^2 - x - 1$.

(d) (5 points) Show that the residue class $[x]$ is invertible in $\mathbb{Q}[x]/(f)$. What is its inverse?

$[x]^{-1} = [x^4]$, as

$[x][x^4] = [x^5] = [1]$.

(can reduce: $[x^4] = [-x^3 - x^2 - x - 1]$).

4. (20 points) Examples.

(a) (5 points) Give your favorite example of a non-commutative ring.

$Mat_{2\times 2}(\mathbb{R})$

(many other examples)

(b) (5 points) Give your favorite example of a ring with no identity element.

$2\mathbb{Z}$

(c) (5 points) Give an example of a ring of characteristic 3 which has more than 3 elements.

$\mathbb{Z}_3[x]$

could also be: $\mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{G}/3\mathbb{G}$, etc.

(d) (5 points) Give an example of a subset S of $\mathbb{Z}$ which is closed under addition and multiplication but is not a subring.

$\mathbb{N} \subseteq \mathbb{Z}$

$(= \{0, 1, 2, \ldots\}$ nonnegative integers)

5. (20 points) Compute 3^{25} mod 15 (hint: use the Chinese remainder theorem, i.e. the isomorphism $\mathbb{Z}_{15} \cong \mathbb{Z}_5 \times \mathbb{Z}_3$).

$3^{25} = 3 \cdot 3^{24} \equiv 0 \mod 3$

$3^4 \equiv 1 \mod 5$ (FLT)

$\Rightarrow 3^{4 \cdot 6} = (3^4)^6 \equiv 1^6 \equiv 1 \mod 5$

$\Rightarrow 3^{25} = 3^{24} \cdot 3 \equiv 1 \cdot 3 \equiv 3 \mod 5$

By CRT, there is a unique residue of 15 $x \in \mathbb{Z}_{15}$ with

$x \equiv 0 \mod 3$

$x \equiv 3 \mod 5$,

and one finds this unique residue to be $x \equiv 3$

$\therefore 3^{25} \equiv 3 \mod 15$

6. (20 points) True/False (give a short argument, about one sentence):

(a) If $S \leq R$ is a subring and S has an identity element then R also has an identity element.

F. Consider $S = R_1 \times R_2$ such that R_1 does not have an identity element and R_2 does (e.g. $2\mathbb{Z} \times \mathbb{Z}$). Let $R = \{0\} \times R_2 \subseteq S$. Then R has identity, S does not.

(b) Every ring with identity for which $1_R = 0_R$ is isomorphic to the zero ring.

T. Proved in class.

(c) Every ring of characteristic 5 has finitely many elements.

F. Consider $\mathbb{Z}_5[x]$

(or $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \cdots$ infinitely many times: sequences of residues mod 5)

(d) In $\mathbb{Z}_5[x]$, the product of a polynomial of degree 3 and a polynomial of degree 4 must have degree 7.

T, as $\mathbb{Z}_5$ is a domain.

(e) There is a ring of order n for every positive integer n.

T: take $\mathbb{Z}_n$

($\mathbb{Z}_1 = \{0\}$ for $n=1$, still a ring)