Exam #3 Solutions

1a. integral domain is a commutative ring w/ identity and no zero divisors.

b. If $a, b \neq 0$ but $ab = 0$ then a and b are zero divisors.

c. The characteristic of R is the smallest $n \in \mathbb{Z}^+$ such that $n \cdot r = 0$ $\forall r \in R$. If no such n exists we say R has characteristic zero.

d. An ideal is a additive subgroup $N \leq R$ such that $rn, nr \in N$ $\forall n \in N, r \in R$.

e. $\phi: R \to R'$ is a ring homomorphism if:

$$\phi(xy) = \phi(x)\phi(y)$$
$$\phi(x+y) = \phi(x) + \phi(y) \qquad \forall x, y \in R$$

2. a. F ex. $\mathbb{Z}/10\mathbb{Z}$

b. F Let $R = \mathbb{Z}/4\mathbb{Z}$ and $N = \{0, 2\}$, $R/N \cong \mathbb{Z}/2\mathbb{Z}$.

c. T

d. F

e. F

f. F

g. F $\mathbb{Q}$ is

h. F $\mathbb{Z}_{20}$ is not a field

3

a. $n^1 = n \in N$ so $N \subseteq \sqrt{N}$

b. Let $a, b \in \sqrt{N}$ so $a^n, b^m \in N$ for some $n, m \in \mathbb{Z}^+$.

$$(-a)^n = (-1)^n \cdot a^n = \pm a^n \in N \text{ since } a^n \in N$$

$$(a+b)^{n+m} = a^{n+m} + \cancel{\pm} a^{n+m-1} b^m + \dots + b^{n+m}$$

all terms have either a^n or b^m

and since N is an ideal w/ $a^n, b^m \in N$

$$a^n \cdot a^k b^s \in N$$

$$a^\ell b^t b^m \in N$$

Thus $(a+b) \in \sqrt{N}$ so $\sqrt{N}$ is a subgroup

Now $(ra)^n = r^n a^n$ since R is comm, but $a^n \in N$

so $r^n a^n \in N$ so $(ra)^n \in N$ so $ra \in \sqrt{N}$.

$ra = ar$ so $ar \in \sqrt{N}$. Thus $\sqrt{N}$ is an ideal

c. Let $a \in \sqrt{\sqrt{N}}$. Then $a^n \in \sqrt{N}$ for some n by def.

But then $(a^n)^m = a^{nm} \in N$ by def of $\sqrt{\ }$.

Thus $a \in \sqrt{N}$. Thus $\sqrt{N} \supseteq \sqrt{\sqrt{N}}$.

But $\sqrt{N} \subseteq \sqrt{\sqrt{N}}$ by part a

So $\sqrt{N} = \sqrt{\sqrt{N}}$.

3. $R = \mathbb{Z}$ $N = 8\mathbb{Z}$ $\sqrt{N} = 2\mathbb{Z}$

4. Let $x, y \in \ker \phi$, $r \in R$,

$$\phi(x+y) = \phi(x) + \phi(y) = 0+0 = 0 \quad \text{so } x+y \in \ker \phi$$
$$\phi(x-y) = \phi(x) - \phi(y) = 0-0=0 \quad \text{so } x-y \in \ker\phi$$
$$\phi(rx) = \phi(r)\phi(x) = \phi(r)\cdot 0 = 0 \text{ so } rx \in \ker\phi$$
$$\phi(xr) = \phi(x)\phi(r) = 0\phi(r) = 0 \text{ so } xr \in \ker \phi$$

Thus $\ker\phi$ is an ideal.

5. Let $p(x) = a_0 + a_1x + \dots + a_nx^n$ with $a_i \in \mathbb{Z}$, $a_n \neq 0$.

If $p \nmid a_n$, $p \mid a_i$ for $i<n$ and $p^2 \nmid a_0$ then

$p(x)$ is irreducible over $\mathbb{Q}$

$x^3 + 6x^2 - 12$ irred using $p = 3$

$6x^4 - 3x^2 - 9x + 3$ No prime works

$5x^3 + 10x - 6$ irr. using $p = 5$

6.

a. $\phi(p^2) = p^2 - p$ $\qquad \phi(pq) = (p-1)(q-1)$

b. $a^{\phi(n)} \equiv 1 \bmod n$ if $\gcd(a,n) = 1$

c. $37 \equiv 5 \bmod 8$ so and $\phi(8) = 4$ so $5^4 \equiv 1 \bmod 8$

$$37^{50} \equiv 5^{50} \equiv 5^{48} \cdot 5^2 \equiv 5^2 \equiv \boxed{1 \bmod 8}$$

7. a. $\mathbb{Z}$ $\qquad$ b. $2\mathbb{Z}$ $\qquad$ c. $M_n(\mathbb{Z})$

d. $2\mathbb{Z}/6\mathbb{Z}$

8. a. Let $x, y \in U(R)$ so $\exists\ x^{-1}, y^{-1}$ with
$xx^{-1} = x^{-1}x = 1$
$yy^{-1} = y^{-1}y = 1$

Notice $xy \cdot y^{-1}x^{-1} = xx^{-1} = 1$
$y^{-1}x^{-1}xy = y^{-1}y = 1$ so xy is invertible with inverse $y^{-1}x^{-1}$.

Clearly $(x^{-1})^{-1} = x$ so x^{-1} is invertible. Thus $xy \in U(R)$
$x^{-1} \in U(R)$.

Assoc. law holds for all of R.

$1 \in U(R)$ so identity.

Hence $U(R)$ is a group under $\cdot$

8.b

$U(\mathbb{Z}) = \pm 1 \qquad U(\mathbb{Q}) = \mathbb{Q}^*$

$U(\mathbb{Z}/n\mathbb{Z}) = \{a + n\mathbb{Z} \mid \gcd(a,n) = 1\}$

$U(\mathbb{Z}[\omega]) = \pm 1$

$U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$