due April 30 | Homework Set 13 (section 5.3 – 6.2) | Name: ____________

When writing a proof, be sure to cite all of the properties, theorems, corollaries, and definitions you use. Be sure to write all of your answers in complete sentences (even the non-proof questions).

1. Answer the following (non-proof) questions:
   a. Determine whether the given ring is a field

3 i. $\mathbb{Z}_3[x]/\langle x^3+2x^2+x+1\rangle$

field b/c x^3+2x^2+x+1 is irreducible (by Thrm 5.10)

3 ii. $\mathbb{Z}_5[x]/\langle 2x^3-4x^2+2x+1\rangle$

not a field b/c $2x^3-4x^2+2x+1=(x-2)(2x^2+2)$ in $\mathbb{Z}_5[x]$

3 iii. $\mathbb{Z}_2[x]/\langle x^4+x^2+1\rangle$

not a field b/c $x^4+x^2+1=(x^2+x+1)^2$ in $\mathbb{Z}_2[x]$

6 b. List the distinct principal ideals of the ring $\mathbb{Z}_{12}$.

$\langle 0\rangle=\{0\}$
$\langle 1\rangle=\mathbb{Z}_{12}$
$\langle 2\rangle=\{0,2,4,6,8,10\}$
$\langle 3\rangle=\{0,3,6,9\}$
$\langle 4\rangle=\{0,4,8\}$
$\langle 6\rangle=\{0,6\}$

5 c. Explain why $\langle 4,6\rangle=\langle 2\rangle$ in $\mathbb{Z}$.

pick $a\in\langle 4,6\rangle$. Then $a=4k+6t=2(2k+3t)\in\langle 2\rangle$ for some $k,t\in\mathbb{Z}$.
Hence, $\langle 4,6\rangle\subseteq\langle 2\rangle$.
Now, $\langle 4,6\rangle=\{4k+6t\mid k,t\in\mathbb{Z}\}$ by Theorem 1.3, $\gcd(4,6)=2$ is the smallest positive integer in $\langle 4,6\rangle$, and there are $u,v\in\mathbb{Z}$ such that $2=4u+6v$.
pick $b\in\langle 2\rangle$. Then $b=2n=(4u+6v)n=4(un)+6(vn)\in\langle 4,6\rangle$ for some $n\in\mathbb{Z}$.
Hence, $\langle 2\rangle\subseteq\langle 4,6\rangle$. Therefore, $\langle 2\rangle=\langle 4,6\rangle$.

2. Let I and J be ideals in R. Prove that the set $I+J=\{a+b\mid a\in I, b\in J\}$ is an ideal in R that contains both I and J.

Let I and J be ideals in ring R. Consider $I+J$. Obviously, $I\subseteq I+J$ and $J\subseteq I+J$ (in the definition, let $b=0_R$ and $a=0_R$, respectively). Since $0_R\in I$ and $0_R\in J$, we see that $0_R=0_R+0_R\in I+J$. Pick $r\in R$; $t,s\in I+J$. Then there are $a,i\in I$ and $b,j\in J$ such that $t=a+b$ and $s=i+j$.
Consider: $t-s=(a+b)-(i+j)=(a-i)+(b-j)\in I+J$ since $a-i\in I$ and $b-j\in J$.
Also, $rt=r(a+b)=ra+rb\in I+J$ since $ra\in I$ and $rb\in J$.
Both of these last two conditions are true because I and J are ideals.
Thus, by the Ideal Test, $I+J$ is an ideal.

3. If $\gcd(m, n) = 1$ in $\mathbb{Z}$, prove that $\langle m \rangle \cap \langle n \rangle$ is the ideal $\langle mn \rangle$.

Let $m, n \in \mathbb{Z}$ such that $\gcd(m,n) = 1$. Recall that $\langle m \rangle = \{m \cdot a \mid a \in \mathbb{Z}\}$ and $\langle n \rangle = \{n \cdot b \mid b \in \mathbb{Z}\}$ and $\langle mn \rangle = \{mn \cdot c \mid c \in \mathbb{Z}\}$.

Let $k \in \langle m \rangle \cap \langle n \rangle$. Then $k = ma$ and $k = nb$ for some $a, b \in \mathbb{Z}$. Hence, n divides k. Since $\gcd(m,n) = 1$, by Theorem 1.5, n divides a. By definition, there exists an integer t such that $a = nt$. Thus, $k = mnt$, meaning that $k \in \langle mn \rangle$.

Let $l \in \langle mn \rangle$. Then $l = mnc$ for some $c \in \mathbb{Z}$. Hence $l \in \langle m \rangle$ and $l \in \langle n \rangle$. Yeilding that $l \in \langle m \rangle \cap \langle n \rangle$.

4. Let I and K be ideals in a ring R, with $K \subseteq I$. Prove that $I/K = \{a + K \mid a \in I\}$ is an ideal of the quotient ring R/K.

Let I and K be ideals of ring R with $K \subseteq I$. Since $0_R \in I$, $0_R + K \in I/K$.
Pick $a+K, b+K \in I/K$. Then $(a+K) - (b+K) = (a-b) + K \in I/K$ since $a - b \in I$.
Pick $r + K \in R/K$. Then $(r+K)(a+K) = ra + K \in I/K$ and $(a+K)(r+K) = ar + K \in I/K$ since $ra, ar \in I$.
Thus, I/K is an ideal of R/K by the Ideal Test.

5. Suppose that I and J are ideals of a ring R, and let $f: R \to R/I \times R/J$ be the function defined by $f(a) = (a + I, a + J)$.

a. Prove that f is a homomorphism of rings.

10

Suppose I and J are ideals of ring R. Define $f: R \to R/I \times R/J$ by $f(a) = (a+I, a+J)$ for any $a \in R$. Pick $a, b \in R$. Then

$$f(a+b) = ((a+b)+I, (a+b)+J) = ((a+I)+(b+I), (a+J)+(b+J)) = (a+I, a+J) + (b+I, b+J) = f(a)+f(b)$$

and

$$f(ab) = (ab+I, ab+J) = ((a+I)(b+I), (a+J)(b+J)) = (a+I, a+J)(b+I, b+J) = f(a)f(b).$$

Thus, f is a homomorphism.

5

b. Is f surjective?

No, because $(a+I, b+J) \in R/I \times R/J$ where $a \neq b$ in R but no element in R, say c, will give $f(c) = (a+I, b+J)$.

5

c. What is the kernel of f?

$$\ker(f) = \{r \in R \mid f(r) = (0_R + I, 0_R + J)\} = I \cap J$$

since $r + I = 0_R + I$ exactly when $r \in I$ similarly $r + J = 0_R + J$ when $r \in J$.