Name ____ Fields and Rings, Test 2, Fall 2017

1) Prove the following theorems:

- T1
- T3
- T8
- T9
- T12
- T14a
- T16a
- T17a

Theorem T1: Let a, b, and c be elements of a ring R. If $a + b = a + c$, then $b = c$.

Assume $a + b = a + c$
a has an additive inverse, call it d.
Call the additive identity e.
$\therefore d + a + b = d + a + c$
$\therefore e + b = e + c$
$\therefore b = c$

Theorem T3: Let R be a ring. If $a + 0_1 = a$ and $a + 0_2 = a$ for all elements $a \in R$, then $0_1 = 0_2$.

Assume $a + 0_1 = a$ and $a + 0_2 = a$ for all elements $a \in R$.
Therefore for some particular element $b \in R$, $b + 0_1 = b$ and $b + 0_2 = b$.
$\therefore b + 0_1 = b + 0_2$
$\therefore 0_1 = 0_2$

Theorem T8: Let R be a ring. If R has a multiplicative identity, then it is unique.

Let 1_a and 1_b be multiplicative identities.
$\therefore 1_a = 1_a 1_b = 1_b$

Theorem T9: Let R be an integral domain and suppose $a \neq 0$. If $ab = ac$, then $b = c$.

Assume $ab = ac$
$\therefore ab - ac = 0$
$\therefore a(b - c) = 0$
$\therefore b - c = 0$ (This is because R is an integral domain and $a \neq 0$)
$\therefore b = c$

Theorem T12: Let p be a prime number and $0 \neq x \in \mathbb{Z}_p$. Then $x^{p-1} = 1$ in $\mathbb{Z}_p$.

Let $0 \leq a, b < p$. Then for $0 < n < p$ we know that if $an = ab$, then $a = b$. Hence the two sets of numbers below give all nonzero elements of $\mathbb{Z}_p$.

$$\{1, 2, 3, \dots, p-1\}$$
$$\{x, 2x, 3x, 4x, \dots, (p-1)x\}$$

$\therefore 1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv x \cdot 2x \cdot \cdots \cdot (p-1)x$
$\therefore (p-1)! \equiv x^{p-1}(p-1)!$
$\therefore 1 \equiv x^{p-1}$

Theorem T14a: Let R be a commutative ring with identity. Fix two elements $a, b \in R$. If $\langle a \rangle \subseteq \langle b \rangle$, then $a = bt$ for some $t \in R$.

Assume $\langle a \rangle \subseteq \langle b \rangle$
$\therefore a \in \langle b \rangle$
$\therefore a = bt$ for some $t \in R$

Theorem T16a: Let R be an integral domain and let $r, s \in R$. If $\langle r \rangle = \langle s \rangle$, then r and s are associates.

Assume $\langle r \rangle = \langle s \rangle$

$$\therefore r \in \langle s \rangle$$

$\therefore r = sk$ for some $k \in R$

$$\therefore s \in \langle r \rangle$$

$\therefore s = rk_2$ for some $k_2 \in R$

$$\therefore r = rk_2k$$
$$\therefore k_2k = 1$$

Therefore r and s are associates. (Because $r = sk$ where k is a unit)

Theorem T17a: Let R be a commutative ring with unity. If R is a field then its only ideals are $\{0\}$ and R itself.

Assume R is a field.
Let I be an idea of R.
If $I \neq \{0\}$, then there is some nonzero element of I, call it x.
Because R is a field, x^{-1} exists.
$\therefore x^{-1} \cdot x \in I$
$\therefore 1 \in I$
$\therefore I = R$

2) Let R be a commutative ring and S and T ideals of R. Define $J \coloneqq \{a + b | a \in S, b \in T\}$. Prove that J is an ideal of R.

We must show that J is a subring that satisfies the stronger multiplication property: $xr \in J$ whenever $x \in J$ and $r \in R$.

Proof that $J \neq \emptyset$:
$0 = 0 + 0 \in J$

Proof that $x - y \in J$ whenever $x, y \in J$:
$x = a + b$ for some $a \in S$ and $b \in T$
$y = c + d$ for some $c \in S$ and $d \in T$
$x - y = a + b - (c + d) = (a - c) + (b - d) \in J$ because $a - c \in S$ and $b - d \in T$.

Proof that $xr \in J$ whenever $x \in J$ and $r \in R$:
$x = a + b$ for some $a \in S$ and $b \in T$
$xr = ar + br \in J$ because $ar \in S$ and $br \in T$.

3) Compute $4a$ and a^2 in $\mathbb{Q}[x]$ for $a = 1 + 3x^2$.

$4a = 4(1 + 3x^2) = 4 + 12x^2$
$a^2 = (1 + 3x^2)^2 = 1 + 6x^2 + 9x^4$

4) Compute $4a$ and a^4 in $\mathbb{Z}_7$ for $a = 2$.

$4a = 4 \cdot 2 = 1$
$a^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 4 \cdot 2 \cdot 2 = 1 \cdot 2 = 2$

5) Find all the subrings of $\mathbb{Z}_{12}$.

$\{0\}, \langle 6 \rangle, \langle 4 \rangle, \langle 3 \rangle, \langle 2 \rangle, \mathbb{Z}_{12}$

6) Consider $\varphi: \mathbb{Z}: \to 2\mathbb{Z}$ given by $\varphi(n) = 2n$. Explain why φ is not a ring homomorphism.

It does not satisfy the multiplication property. Consider, for instance:
$\varphi(3 \cdot 3) = \varphi(9) = 18$
$\varphi(3)\varphi(3) = 6 \cdot 6 = 36$

7) Write the number $e^{\frac{i\pi}{4}}$ in rectangular coordinates as $a + bi$.

$$e^{\frac{i\pi}{4}} = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

8) Show that in $\mathbb{Q} \times \mathbb{Z}$, the elements $(2, -1)$ and $(4,1)$ are associates.

$$(2, -1) \cdot (2, -1) = (4,1)$$

$(2, -1)$ is a unit because $2 \cdot \frac{1}{2} = 1$ in $\mathbb{Q}$ and $-1 \cdot -1 = 1$ in $\mathbb{Z}$.

9) Explain why a field is always a PID, practically by default.

A field has only two ideals (Theorem 17), each of those ideas are principle.

10) Give a nice description of the ideal $\langle\sqrt{7}\rangle$ in the ring $\mathbb{Z}[\sqrt{7}]$.

$$\langle\sqrt{7}\rangle = \{\sqrt{7}x | x \in \mathbb{Z}[\sqrt{7}]\} = \{\sqrt{7}a + \sqrt{7}(b\sqrt{7}) | a, b \in \mathbb{Z}\} = \{7b + \sqrt{7}a | a, b \in \mathbb{Z}\}$$

This is the set of everything in $\mathbb{Z}[\sqrt{7}]$ that has a rational part divisible by 7.

11) Factor $x^3 - 2$ into irreducibles in $\mathbb{Q}[x]$.

$$x^3 - 2$$

If we look at its roots, we get $x^3 = 2$. One solution over $\mathbb{R}$ is $\sqrt[3]{2}$. The other two solutions are complex, oriented uniformly over the circle of radius $\sqrt[3]{2}$ on the complex plane. None of those three roots are rational, so this polynomial cannot be factored.

12) Let $\mathbb{F}$ be a field. Could the ring $\mathbb{F}[x]$ be a field? Why or why not?

No, because x is not invertible.

13) Use the ring $R = \mathbb{Z}[\sqrt{2}]$ for this problem. Simplify the ideal $\langle 3 + 8\sqrt{2}, 7\rangle$ in this ring.

$$\langle 3 + 8\sqrt{2}, 7\rangle$$

First note that because $7 \in \langle 3 + 8\sqrt{2}, 7\rangle$, so also $7\sqrt{2}$ is.
$3 + 8\sqrt{2} = (3 + \sqrt{2}) + 7\sqrt{2}$
$\therefore \langle 3 + 8\sqrt{2}, 7\rangle = \langle 3 + \sqrt{2}, 7\rangle$

Now note that $(3 + \sqrt{2})(3 - \sqrt{2}) = 9 - 2 = 7$. Hence 7 is a multiple of $3 + \sqrt{2}$ and is thus redundant.
$\therefore \langle 3 + \sqrt{2}, 7\rangle = \langle 3 + \sqrt{2}\rangle$

$\therefore \langle 3 + 8\sqrt{2}, 7\rangle = \langle 3 + \sqrt{2}\rangle$