Math 250/M2/Fall ’13 The Halloween Midterm
Burger

HP Grade ____ Name ___________KEY___________________

(20pts)

1. In Z[i], completely factor the element 13+5i into irreducible factors.

$(9+4i)(1+i) = 9 + 13i - 4 = 5$

$(9-4i)(1+i) = 9 + 9i - 4i + 4$ i.

So $\boxed{13+5i = (9-4i)(1+i)}$.

(20pts)

2. Given that $\phi: R \to S$ is a ring isomorphism, prove that if R is an integral domain, then so is S.

Proof. Suppose, by contradiction, that S has zero divisors.
Then we have $\phi(0_R) \overset{\text{hom.}}{=} 0_S = z\cdot w$ for some $z, w \in S$, $z, w \neq 0$.
Since ϕ is onto, $z = \phi(x)$ and $w = \phi(y)$ for some $x, y \in R$.
So we have $\phi(x\cdot y) = 0_S$ and $\phi(0_R) = 0_S$.
Since ϕ is one-to-one, we conclude that $x \cdot y = 0_R$.
Since R is an integral domain, $x = 0$ or $y = 0$.
Assume WLOG that $x \neq 0$. Then $y = 0$. Cool!
Then we have $\phi(y) = \phi(0_R) = w \neq 0_S$, a contradiction, since ϕ is a homomorphism.
Thus, S has no zero divisors.
Now, since R is an integral domain, R is a commutative ring, and since ϕ is a homomorphism, we have

$$\phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x).$$

Since ϕ is onto, this is true $\forall x, y \in S$. ← *A KEY POINT*
Thus, S is commutative.
Therefore, S is an integral domain. □

Math 250/M2/Fall ’ 13 The Halloween Midterm

Burger

(30pts) 

3. Let $f(x) = x^4 + 1 \in \mathbb{Z}_3[x]$:

   a. Find the least number of extension fields needed to factor $f(x)$ into **linear** terms. (Careful as $f(x)$ maybe be reducible in $\mathbb{Z}_3[x]$!)

   b. How many elements are in the final extension you found?

(a) $f(0) = 1 \neq 0$, $f(1) = 2 \neq 0$, and $f(2) = 17 = 2 \neq 0$.

So if f factors, it is of the form $(ax^2+bx+c)(dx^2+ex+g)$.

Then $x^4+1 = (ad)x^4 + (ae+bd)x^3 + (ag+be+cd)x^2 + (bg+ce)x + cg$.

So $ad = cg = 1$ and $ae+bd = ag+be+cd = bg+ce = 0$.

$a=1 \Rightarrow d=1$.

$c=1 \Rightarrow g=1 \Rightarrow bg+ce = b+e=0 \Rightarrow b=-e \Rightarrow ag+be+cd = 1-e^2+1=0 \Rightarrow e^2=2$, impossible.

$c=2 \Rightarrow g=2 \Rightarrow bg+ce = 2b+2e=0 \Rightarrow b=-e \Rightarrow ag+be+cd = 2-e^2+2=0 \Rightarrow e^2=1$

Wait... $x^4+1 = (x^2+x+2)(x^2+2x+2)$, so x^4+1 is <u>not</u> irreducible. $e=2, b=1$

Well, going on anyway...

(b) Let $q_1(x) = x^2+x+2$ and $q_2(x) = x^2+2x+2$.

$q_1(0) = 2 \neq 0$, $q_1(1) = 4 = 1 \neq 0$, and $q_1(2) = 8 = 2 \neq 0$, so $q_1(x)$ is irreducible in $\mathbb{Z}_3$, and

$q_2(0) = 2 \neq 0$, $q_2(1) = 5 = 2 \neq 0$, and $q_2(2) = 10 = 1 \neq 0$, so $q_2(x)$ is irreducible in $\mathbb{Z}_3$.

Let $F = \mathbb{Z}_3[x]/\langle q_1(x)\rangle$. Then $q_1(x)$ has a root, say α, in F.

$$\begin{array}{r|l} & 1 \quad (1+\alpha) \\ 1 \ (-\alpha) & 1 \quad 1 \quad 2 \\ & 1 \quad (-\alpha) \\ \hline & (1+\alpha) \quad 2 \\ & (1+\alpha) \quad (-\alpha-\alpha^2) \\ \hline & \alpha^2+\alpha+2 = 0 \end{array}$$

$\Rightarrow q_1(x) = (x+2\alpha)(x+(1+\alpha))$.

(3b) (Continued)

Need to Check: α, $1+\alpha$, 2α, $1+2\alpha$, $2+\alpha$, and $2+2\alpha$ to see if they're roots of $q_2(x)$.

$q_2(\alpha) = \alpha^2+2\alpha+2 = \alpha + (\alpha^2+\alpha+2) = \alpha$, no.

$q_2(1+\alpha) = (1+\alpha)^2 + 2(1+\alpha)+2 = \alpha^2+2\alpha+1+2+2\alpha+2 = \alpha^2+\alpha+2 = 0$ ✓

So $1+\alpha$ is a root of $q_2(x)$. So $x-(1+\alpha) = [x+(2+2\alpha)] \mid q_2(x)$.

$$\begin{array}{r|lll} & & 1 & \alpha \\ \hline 1 \ (2+2\alpha) & 1 & 2 & 2 \\ & -1 & (2+2\alpha) & \\ \hline & & \alpha & 2 \\ & & \alpha & 2\alpha+2\alpha^2 \\ \hline & & & \alpha^2+\alpha+2=0 \end{array}$$

$\Rightarrow q_2(x) = (x+(2+2\alpha))(x+\alpha)$.

Awesome!

Putting it all together, $x^4+1 = (x+2\alpha)(x+(1+\alpha))(x+(2+2\alpha))(x+\alpha)$ in F.

So the least number of extension fields required is $\boxed{1}$.

(3c) F is $\mathbb{Z}_3[x]$ mod a degree-2 polynomial, so its elements are all linear.

Thus, there are $3^2 = \boxed{9}$ elements in F.

(30pts)

4. For the ideal in $\mathbb{Z}[i]$ defined by:
   $I = \{a \cdot (5-i) + b \cdot (18+2i) : a, b \in \mathbb{Z}[i]\}$ find a and b which generate the element $958 + 958i \in I$.

$$\frac{18+2i}{5-i} = \frac{18+2i}{5-i} \cdot \frac{5+i}{5+i} = \frac{90+28i-2}{26} = \frac{88+28i}{26} = \frac{44}{13} + \frac{14}{13}i \; ; \; q_1 = 3, q_2 = 1 \Rightarrow q = 3+i.$$

$$18+2i = \underbrace{(5-i)(3+i)}_{15+2i+1} + 2.$$

$$\frac{5-i}{2} = \frac{5}{2} - \frac{1}{2}i \; ; \; q_1 = 2, q_2 = 0 \Rightarrow q = 2.$$

$$5-i = 2 \cdot 2 + (1-i).$$

Now, $\frac{958+958i}{1-i} = \frac{958+958i}{1-i} \cdot \frac{1+i}{1+i} = \frac{958+1916i-958}{2} = 958i$, so $(1-i) \mid (958+958i)$, so there is a solution, and $958+958i = (1-i)958i$.

$$1-i = 5-i-2 \cdot 2 = (5-i) - 2\left[(18+2i) - (5-i)(3+i)\right]$$
$$= (5-i)\left[1+2(3+i)\right] + (18+2i)[-2]$$
$$= (5-i)(7+2i) + (18+2i)(-2).$$

So $958+958i = 958i(1-i) = 958i\left[(5-i)(7+2i) + (18+2i)(-2)\right]$
$$= (5-i)(-1916+6706i) + (18+2i)(-1916i).$$

So $a = -1916 + 6706i$ and $b = -1916i$

NOTE: OTHER ANSWERS ARE POSSIBLE BASED ON WHICH gcd YOU USED, OR EVEN JUST PERFORMING ONE DIVISION AND FINDING A REMAINDER OF 2.