HP	Grade	Name	KEY



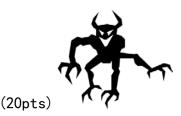
(20pts)

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

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

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

$$56 [13+5i = (9-4i)(1+i)].$$



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 controdiction, that S has zero divisors. Then we have $+(0_R)^{lm} \cdot 0_S = z \cdot w$ for some $z, w \in S$, $z, w \neq 0$. Since \neq is onto, $z = \neq k$) and $w = \neq k$) for some $x, y \in R$. So we have $+(x \cdot y) = 0_S$ and $+(0_R) = 0_S$.

Since \neq is one-to-one, we conclude that $x \cdot y = 0_R$.

Since R is an integral domain, x = 0 or y = 0.

Assume WLDG that $x \neq 0$. Then y = 0.

Then we have $+(y) = +(0_R) = w \neq 0_S$, a controdiction, since \neq is a homomorphism. Thus, \leq has no zero divisors. \leq Now, since R is an integral domain, R is a communicative ring, and since \neq is a homomorphism, we have

 $\phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x)$. Since ϕ is onto, this is true $\forall x,y \in S$. $\leftarrow AKEY POINT$ Thus, S is commutative.

Therefore, S is an integral domain. []



- 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?

So if
$$f$$
 fuctors, it is of the form $(ax^2+bx+c)(dx^2+cx+q)$.

Then $x^4+1=(ad)x^4+[ae+bd]x^2+(aq+be+cd)x^2+(bq+ce)x+cq$.

So $ad=cq=1$ and $ae+bd=aq+be+cd=bq+ce=0$.

 $a=1\Rightarrow d=1$.

 $c=1\Rightarrow q=1\Rightarrow bq+ce=b+e=0\Rightarrow b=-e\Rightarrow aq+be+cd=1-e^2+1=0\Rightarrow e^2=1$, impossible, $c=2\Rightarrow q=2\Rightarrow bq+ce=2b+2e=0\Rightarrow b=-e\Rightarrow aq+be+cd=2-e^2+2=0\Rightarrow e^2=1$

Wait ... $x^4+1=(x^2+x+2)(x^2+2x+2)$, so x^4+1 is not irreducible.

Well, going on anyway ...

(b) Let $q_1(x) = x^2 + x + 2$ and $q_2(x) = x^2 + 2x + 2$. $q_1(0) = 2 + 0$, $q_1(1) = 4 = 1 + 0$, and $q_1(2) = 8 = 2 + 0$, so $q_1(x)$ is irreducible in \mathbb{Z}_3 , and $q_2(0) = 2 + 0$, $q_2(1) = 5 = 2 + 0$, and $q_2(2) = 10 = 1 + 0$, so $q_2(x)$ is irreducible in \mathbb{Z}_3 .

Let $F = \mathbb{Z}_3[x]/(q_1(x))$. Then $q_1(x)$ has a root, sory x, in F. $|f(x)| = \frac{1}{1+x} \frac{1}{2} \frac{1}{1+x} \frac{1}{2} \frac{1}{1+x} \frac{1}{2} \frac{1}{1+x} \frac{1}{2} \frac{1}{1+x} \frac{1}{2} \frac{1}{2} \frac{1}{2} \frac{1}{1+x} \frac{1}{2} \frac$

(36) (Continued)

perdito ant: a, Ita, 2a, It2a, 2ta, and 212a to see if they roots of q2(x).

q+(a) = a2+2a+2 = a+ (a2+a+2) = a, no.

q=(Ita) = (Ita)2+2(Ita)+2 = a2+2a+I+2+2a+2 = 0 \ So Ita is a root of q=(x).

So Ita is a root of q=(x).

$$\frac{1}{(2+2\alpha)} \frac{1}{(1-2\alpha)} \frac{1}{(2+2\alpha)} = \frac{1}{(2+2\alpha)} \frac{1}{(2+2\alpha)}$$

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 F Π .

(3c) F is Zz[x] mod a degree = 2 polynomial, so its elements are all linear.

Thus, there are = [9] elements in F.

(30pts)

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

$$\frac{5-i}{5-i} = \frac{5+i}{5+i} = \frac{90+28i-2}{26} = \frac{88+28i}{26} = \frac{44}{12} + \frac{14}{13}i + \frac{1}{19}i + \frac$$

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