Name: ______________________________ **Problem 1:** ____________ /25

Problem 1(25 points)

(a)(5 points) Construct a field E of finite order 5 and an extension field F of finite order 25.

(b)(5 points) What is the order and isomorphism type of $E^\times$? What is the order and isomorphism type of $F^\times$?

(c)(15 points) Find a generator for $E^\times$ and find a generator for $F^\times$. (**Hint.** You might find it convenient to work out the formulas for the squaring and cubing maps in the quotient group $F^\times/E^\times$.)

(a) $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0, \pm 1, \pm 2\}$, $\mathbb{F}_{25} = \mathbb{F}_5[x]/_{x^2-2} = \{ax+b \mid a, b \in \mathbb{F}_5\}$.

(b) $\mathbb{F}_5^\times \cong \mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_{25}^\times \cong \mathbb{Z}/24\mathbb{Z}$

(c)

$a \in \mathbb{F}_5$	a^2
-2	-1
-1	1
0	0
1	1
2	-1

, So 2 generates $\mathbb{F}_5^\times$.

$\mathbb{F}_{25}^\times/\mathbb{F}_5^\times \cong \mathbb{Z}/6\mathbb{Z}$.

$\bar{x} \cdot \bar{x} \equiv \bar{1} \mod \mathbb{F}_5^\times$

$(\bar{x} - a)(\bar{x} + a) \equiv \bar{x}^2 - a^2 = 2 - a^2 \equiv 1 \mod \mathbb{F}_5^\times$

& $(\bar{x} - a)(\bar{x} - b) = -(a+b)\bar{x} + (ab+2) \equiv \bar{x} - \frac{ab+2}{a+b} \mod \mathbb{F}_5^\times$ if $a+b \neq 0$.

So $(\bar{x}-a)^2 \equiv x - \frac{a^2+2}{2a}$ if $a \neq 0$. So $(\bar{x}-a)^2 = (\bar{x}-a)^{-1} = \bar{x}+a$

$\Leftrightarrow \frac{a^2+2}{2a} = -a \Leftrightarrow 2a^2 - 2 = 0 \Leftrightarrow a = \pm 1$. So $(\bar{x}-1)^3 \equiv 1 \mod \mathbb{F}_5^\times$
$(\bar{x}+1)^3 \equiv 1$

So $\bar{x} - 2$, $\bar{x} + 2$ generate $\mathbb{F}_{25}^\times$ mod $\mathbb{F}_5^\times$. Since $\varphi(24) = \varphi(8)\varphi(3) = 4 \cdot 2 = 8$, the 8 elements $\boxed{a(\bar{x}-2), b(\bar{x}+2),}$ $a, b \in \mathbb{F}_5^\times$ are the generators of $\mathbb{F}_{25}^\times$.

Name: ______________________________ **Problem 2**: ____________ /35

Problem 2(35 points) Let $f(x,y)$ in $\mathbb{C}[x,y]$ be the irreducible polynomial $y^3 - x^5$. Let S be the quotient ring $\mathbb{C}[x,y]/\langle f(x,y)\rangle$. And let R be the subring $\mathbb{C}[x]$. Let F denote the fraction field of S.

(a)(10 points) Prove that $R \subset S$ is an integral ring extension, and find a minimal set of generators for S as an R-module. (**Hint.** What is a basis for $\mathbb{C}[x,y]$ as a free $\mathbb{C}[x]$-module, and which of these basis elements are linearly independent in S?)

(b)(5 points) Using your set of generators, prove that there is no element s in S such that $x \cdot s$ equals y.

(c)(5 points) Consider the monic polynomial $t^3 - x^2$ in $S[t]$. Prove that this polynomial has three distinct roots in the fraction field F. (**Hint**. The denominator of each root is x.)

(d)(5 points) Prove that $t^3 - x^2$ has *no* roots in S.

(e)(10 points) Explain why this implies that S is not a Unique Factorization Domain. (If you have trouble with (a), (b), (c) or (d), but you know a different proof that S is not a UFD, you may explain that proof for partial credit.)

(a) S has free basis $\boxed{1, y, y^2}$ as an R-module. Hence S is a finitely generated R-module, thus an integral extension of R.

(b) $x\cdot(a(x)\cdot 1 + b(x)\cdot y + c(x)\cdot y^2) = (xa(x))\cdot 1 + (xb(x))\cdot y + (xc(x))\cdot y^2$. Since $x(b(x)) = 1$ has no solution in $\mathbb{C}[x]$, there is no s in S with $x\cdot s = y$.

(c) $x^2 = \frac{x^2\cdot x^3}{x^3} = \frac{x^5}{x^3} = \frac{y^3}{x^3} = \left(\frac{y}{x}\right)^3$. So $t^3 - x^2 = (t-\frac{y}{x})(t-\omega\frac{y}{x})(t-\omega^2\frac{y}{x})$, where $\omega = e^{2\pi i/3}$ is a 3^{rd} root of 1.

(d) By (b), there is no s with $x\cdot s = y$. So also no s with $x\cdot s = \omega y$ or $x\cdot s = \omega^2 y$ (otherwise divide by ω, resp. ω^2).

(e) By Gauss's Lemma, if S is a UFD then every factorization of $t^3 - x^2$ over F comes from a factorization over $S \Rightarrow \exists$ a root in S.

Name: ______________________________ **Problem 3:** ____________ /40

Problem 3(40 points) Let R be a commutative ring with 1. Let f be an element in R. And let I be an ideal in R which is disjoint from the subset $f^{\mathbb{N}} := \{1, f, f^2, f^3, \dots\}$. Consider the following subset of R.

$$I' = \{r \in R | \exists f^n \in f^{\mathbb{N}}, f^n r \in I\}.$$

(a)(10 points) Prove that I' is an ideal in R which contains I and which is disjoint from $f^{\mathbb{N}}$.

(b)(15 points) Assume that P is an ideal in R which is maximal among those ideals which are disjoint from $f^{\mathbb{N}}$. Prove that P is a prime ideal: if r is not in P $\cancel{R}$ yet rs is in P $\cancel{R}$, then s is in $\cancel{R}$. P (**Hint.** Since $P + \langle r \rangle$ is an ideal which stricly contains P, what relation does this imply with $f^{\mathbb{N}}$? What happens when you multiply your relation by s?)

(c)(10 points) Now let I be an ideal in R, and let f be an element of R which is not contained in the radical rad(I). Prove that there exists a prime ideal P containing I such that f is not in P.

(d)(5 points) Conclude that the radical of I equals the intersection of all prime ideals P which contain I.

(a) $r_1, r_2 \in I'$. $f^{n_1} r_1, f^{n_2} r_2 \in I \Rightarrow f^{(n_1+n_2)}(r_1+r_2)$

$= f^{n_2}(\underbrace{f^{n_1} r_1}_{I}) + f^{n_1}(\underbrace{f^{n_2} r_2}_{I}) \in I$

So $r_1 + r_2 \in I'$

$r \in I'$, $f^n r \in I$, $f^n(rs) = (f^n r)s \in I \Rightarrow rs \in I'$

So I' is an ideal. For $r \in I$, $f^0 r \in I \Rightarrow r \in I'$!

So $I \subset I'$! If $f^a \in I'$, then $f^n \cdot f^a \in I \Rightarrow f^{n+a} \in I$ which contradicts that $f^{\mathbb{N}} \cap I$ is empty. So I' is disjoint from $f^{\mathbb{N}}$.

(b) Since $P + \langle r \rangle \supsetneq \langle P \rangle$, $\exists n \geq 0$ s.t. $f^n = a \cdot r + p$, $a \in R$, $p \in P$

So $f^n s = a \cdot rs + ps$. But $rs \in P \Rightarrow a \cdot rs \in P$. And $p \in P \Rightarrow ps \in P$.

So $a \cdot rs + ps \in P$. So $s \in P'$! Since $P \subset P'$ & $P' \cap f^{\mathbb{N}} = \emptyset$, & since P is maximal, P equals P'. So $s \in P$.

1c) Since $f \notin rad(I)$, I is disjoint from $f^{\mathbb{N}}$. Let S = set of all ideals $J \subset R$ w/ $I \subset J$ & $J \cap f^{\mathbb{N}} = \emptyset$. For a chain of elements of S (partially ordered by inclusion), the union is an element of S. So by Zorn's Lemma, $\exists$ a maximal element P. And by (b), P is a prime ideal.

1d) Certainly $rad(I) \subset \bigcap_{\substack{P \subset S \\ P \text{ prime} \\ I \subset P}} P$.

And for $f \notin rad(I)$, by the above also $f \notin P \Rightarrow f \notin \bigcap_P P$. So $rad(I)$ equals $\bigcap_P P$.