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 $F^\times / E^\times$.)

\( F_5 = \mathbb{Z}/5\mathbb{Z} = \{0, \pm 1, \pm 2\} \quad F_{25} = F_5[x] / (x^2 - 2) = \{ax + b | a, b \in F_5 \} \)

\( F_5^\times \cong \mathbb{Z}/4\mathbb{Z} \quad F_{25}^\times \cong \mathbb{Z}/24\mathbb{Z} \)

\[ \begin{array}{c|c|c|c}
   a \ mod \ 5 & a^2 \ mod \ 5 \\
   \hline
   0 & 0 \\
   1 & 1 \\
   2 & 4 \\
   3 & 4 \\
   4 & 1
\end{array} \]

So (2) generates $F_5^\times$.

\[ F_{25}^\times / F_5^\times \cong \mathbb{Z}/6\mathbb{Z} \quad \overline{x} \cdot \overline{y} \equiv 1 \ mod \ F_5^\times \]

\( (\overline{x} - \overline{a})(\overline{x} + \overline{a}) \equiv \overline{x}^2 - \overline{a}^2 \equiv 2 - \overline{a}^2 \equiv 1 \ mod \ F_5^\times \)

\& \quad (\overline{x} - \overline{a})(\overline{x} - \overline{b}) = -\overline{a+b}x + (\overline{a+b}) \equiv \overline{x} - \frac{ab+2}{a+b} \ mod \ F_5^\times \]

if $a+b \neq 0$.

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

So $\overline{(x-a)}^2 = (\overline{x-a}) = \overline{x+a}$

\( \iff \frac{a^2+2}{2a} = -a \iff 2a^2 - 2 = 0 \iff a = \pm 1 \quad \therefore \quad \overline{(x-1)}^3 \equiv 1 \ mod \ F_5^\times \)

\( \overline{(x+1)^3} \equiv 1 \)

So $\overline{x-2}, \overline{x+2}$ generate $F_5^\times \ mod \ F_5^\times$. Since $\gamma(24) = \gamma(18) \gamma(13) = 42 = 2$, the 8 elements $[a(\overline{x-2}), b(\overline{x+2})] \quad a, b \in F_5^\times$ are the generators of $F_{25}^\times$. 


Problem 2: Let $f(x, y) = y^3 - x^5$. Let $S$ be the quotient ring $\mathbb{C}[x, y]/(f(x, y))$. 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 $x \cdot s = y$.

(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.)

\[ a) S \text{ has free basis } \left\{ 1, x, y \right\} \text{ as an } R\text{-module.} \]

Hence $S$ is a finitely generated $R$-module, thus an integral extension of $R$.

\[ b) x \cdot (a(x), 1 + b(x) \cdot y + c(x) \cdot y^2) = (x \cdot a(x), 1 + (x \cdot b(x)) \cdot y + (x \cdot c(x)) \cdot y^2). \]

Since $x \cdot (b(x)) = 1$ has no solution in $\mathbb{C}[x]$, there is no $s$ in $S$ with $x \cdot s = y$.

\[ c) x^2 = \frac{x^2 \cdot x^3}{x^3} = \frac{x^5}{x^3} = \frac{y^3}{x} = \left( \frac{y}{x} \right)^3. \]

So $t^3 - x^2 = (t - \frac{x}{x})(t - \frac{x}{x}w)(t - \frac{x}{x}w^2)$;

where $w = e^{2\pi i/3}$ is a 3rd root of 1.

(d) By (b), there is no $s$ with $x \cdot s = y$. So also no $s$ with

$x \cdot s = wy$ or $x \cdot s = wz$ (otherwise divide by $w$, resp. $w^2$).

(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 $S \Rightarrow t$ a root in $S$. 

4
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 $f^N := \{1, f, f^2, f^3, \ldots \}$. Consider the following subset of $R$.

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

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

(b)(15 points) Assume that $P$ is an ideal in $R$ which is maximal among those ideals which are disjoint from $f^N$. Prove that $P$ is a prime ideal: if $r$ is not in $P$ yet $rs$ is in $P$, then $s$ is in $P$. (Hint. Since $P + (r)$ is an ideal which strictly contains $P$, what relation does this imply with $f^N$? 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 $\text{rad}(I)$. 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) $r_1, r_2 \in I' \Rightarrow f^{m+n} (r_1 + r_2) \in I'$

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

So $f^ns = a \cdot rs + ps$. But $rs \in P \Rightarrow a \cdot rs \in P$. And $peP \Rightarrow ps \in P$.

So $a \cdot rs + ps \in P$. So $s \in P$. Since $P$ is maximal, $P$ equals $P'$. So $s \in P'$.
Problem 3 continued

1c) Since \( f \notin \text{rad}(I) \), \( I \) is disjoint from \( f^m \). Let \( S = \) set of all ideals \( JC_R \) or \( I \subseteq J \) & \( J \cap f^m = \emptyset \). 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 \( \text{rad}(I) \subseteq \bigcap P \).

And for \( f \notin \text{rad}(I) \), by the above also \( f \notin P \). So \( \text{rad}(I) \) equals \( \emptyset \).