Math 506 HW7

Rohan Mukherjee

May 7, 2024

Problem 1.

Let I be the ideal in the problem, and assume that $Z(I) \subset S$ is empty. Recall that $Z(I) = \bigcap_{f \in I} Z(f)$. This says that

$$\bigcap_{f \in I} Z(f) = \emptyset$$

And so,

$$\bigcup_{f \in I} Z(f)^c = S$$

Since each of the $Z(f)$ are closed (being the preimage of the closed set $\{0\}$ under the continuous function f), we know that each $Z(f)^c$ is open and hence $\{Z(f)\}_{f \in I}$ is an open cover of S. Since S is compact there is a finite subcover

$$S = \bigcup_{i=1}^{n} Z(f_i)^c$$

Taking complements, we get that

$$Z(f_1, \dots, f_n) = \emptyset$$

I claim that this means that I has a unit, and hence is not proper. First, notice that if f is a continous function without any roots, then $1/f$ is also continuous, and hence f is a unit. Thus every $f \in I$ must have at least one root. Under the above hypothesis, we see that $\sum_{i=1}^{n} f_i^2$ has no roots (the only way this could be 0 is if $f_i(x) = 0$ for all $1 \leq i \leq n$), which

contradicts that I is proper, completing the proof. Let I be the ideal of functions that vanish at 0. I is maximal because it is the kernel of the surjective map $f \mapsto f(0) \in \mathbb{R}$ where we note that $\mathbb{R}$ is a field. Since the $I \subset \sqrt{I}$, either $\sqrt{I}$ is all of R or just I, and it is clearly the second case. Now define

$$J = \left\{ f(x) \in R \mid \lim_{x \to 0^+} \left| \frac{f(x)}{x^k} \right| = 0 \right\}$$

We see that J does not contain x, since x/x^2 does not go to 0 as x goes to 0. Defining

$$f(x) = \begin{cases} e^{-1/x} & \text{if } 0 < x \leq 1 \\ 0 & \text{if } x = 0 \end{cases}$$

One notices that

$$\lim_{x \to 0^+} \frac{e^{-1/x}}{x^k} = \lim_{u \to \infty} u^k e^{-u} = 0$$

Thus J is nonempty. Finally, if $f^n \in J$, then

$$\lim_{x \to 0^+} \left| \frac{f(x)}{x^k} \right| = \lim_{x \to 0^+} \sqrt[n]{\left| \frac{f^n(x)}{x^{nk}} \right|} = \sqrt[n]{\lim_{x \to 0^+} \left| \frac{f^n(x)}{x^{nk}} \right|} = 0$$

Since $x \mapsto \sqrt[n]{x}$ is continuous. This shows that $f \in J$ as well so that J is radical, and not equal to the previous I. It is indeed clear by the definition of J that $Z(J) \supseteq \{0\}$. Similarly, the example function provided to show that J is nonempty has no other zeros in $[0, 1]$, thus we have that $Z(J) = \{0\}$. The same function can show that $Z(I) = \{0\}$, but I and J are distinct radical ideals, completing the proof.

Problem 2.

Recall that for any ring R and $a, b \in R$, we have that $(a, b) = (a, b + ra)$. Suppose on the contrary that $I = (x^n, x^{n-1}y, \ldots, y^n) = (p_1, \ldots, p_n)$ for some polynomials $p_1, \ldots, p_n \in k[x, y]$. We see first that every $k[x, y]$ linear combination of the terms in I has every monomial term with degree $\geq n$. By this observation we must have that every monomial term in each of the p_i has degree at least n. If every p_i had every term at least $n + 1$, then the above equality certainly does not hold. We consider equations of the form:

$$\sum q_i p_i = x^{n-i} y^i$$

for $0 \leq i \leq n$. We match the terms of degree n on each side to see that at least one of the q_i must just be in k, where the associated p_i has a term of degree precisely n. By looking at all the p_i with $\deg q_i = 0$ with a term of degree precisely n, we first match the terms of degree precisely n on both sides, and then see that the rest of terms are just being used to cancel out the higher order terms of the p_i. By repeating this for every i, we can replace the p_i with only the degree n terms of each p_i, dropping the p_i with no terms exactly n. Clearly, the $x^{n-i}y^i$ are all the monomial terms of degree precisely n. In this way we get the above relation where each of the p_i have only terms of degree precisely n. We write

$$\sum q_i p_i = x^{n-i}y^i$$

Again at least one of the q_i has degree precisely 0, i.e. is a constant. Assuming that none of the p_i are just 0, we would see that if any of the q_i have degree > 0, then we would need a q_j of the same degree to cancel out the new terms added by the first q_i. Since we can again just throw out polynomial terms that have degree $> n$ because they are going to be 0 anyways, we only keep the $q_i \in k$. We do this for each equation. If we had an equation of the form

$$\sum a_i x^{n-i}y^i = 0$$

By matching coefficients on both sides we see that each a_i must equal 0. In this way, $\text{span}_k \left\{x^n, x^{n-1}y, \ldots, y^n\right\}$ is an $n+1$-dimensional vector space over k. We are now left with n elements p_i that k-span the $n+1$-dimensional vector space $\text{span}_k \left\{x^n, x^{n-1}y, \ldots, y^n\right\}$. This is a contradiction, which completes the proof.

Problem 3.

Suppose that $z \in R$ is a prime element. Then $z \cdot \bar{z} = N(z)$ where $N(z) \in \mathbb{N}$. Thus $N(z)$ has a prime factorization $p^{\alpha}q_2^{\alpha_2} \cdot \cdots \cdot q_n^{\alpha_n}$ over $\mathbb{Z}$. Since z is prime it follows that $z \mid p$. If p is prime in R then z is an associate of p. Otherwise, $p = zw$ where w is not a unit (otherwise p would be prime, being an associate of the prime z). Notice that if $N(a) = 1$ then $a\bar{a} = 1$ so certainly a is a unit in R. Thus $N(z), N(w) > 1$. Now, as $p = zw$ we have that $N(z)N(w) = N(p) = p^2$. By the above this means that $N(z) = N(w) = p$. Thus z has prime norm in this case.

Now let $p \equiv 3 \bmod 4$. If p were somehow reducible as $p = zw$, then we would have $N(z) = p$. Writing $z = a + bi$, we have that $a^2 + b^2 = p$. Now, notice that the squares mod 4 are either 0 or 1, because $0^2 = 0$, $1^2 = 1$, $2^2 = 4 = 0$ and $3^2 = 9 = 1$. In any case, $a^2 + b^2$ is either 0, 1, or 2 mod 4, a contradiction. So p is prime in this case.

Let σ be a generator for the cyclic group $(\mathbb{Z}/p)^{\times}$ of order $p-1$. Since $4 \mid p-1$, we know

that $\sigma^{(p-1)/4}$ has order 4. Thus in particular $\sigma^{(p-1)/2}$ has order 2 and as $\mathbb{Z}/p[x]$ is a field and $x^2 - 1 = 0$ has only two solutions -1 and 1, we see that $\sigma^{(p-1)/4}$ squares to -1. Thus there is an $x \in \mathbb{Z}$ with $x^2 + 1 = p \cdot k$ for some $k > 0$. Suppose per the contrary that p is prime. Then we know that $(1 + ix)(1 - ix) = 1 + x^2 = p \cdot k$. Since p is prime, we know that $p \mid 1 + i \cdot x$ or $1 - i \cdot x$. This says that $p \mid 1$, a contradiction, so p is not prime and since R is a UFD not irreducible. Thus there is some z, w so that $p = z \cdot w$. We showed above that this must mean that $N(z) = p$, which shows that p is of the form $a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Last but not least, we notice that $2 = (1 + i)(1 - i)$. Thus 2 is not prime in R, which classifies all the primes of R.