ASSIGNMENT 1

JONAS TREPIAKAS

Exercise 0.1 (1)**.** *Proof.* (i) We claim that $\left(x^2+1\right)$ is a radical, prime and maximal ideal in $\mathbb{R}[x]$. This can be seen by noting that $\mathbb{R}[x]/\left(x^2+1\right) \cong \mathbb{C}$ which is a field. Hence $\left(x^2+1\right)$ is maximal. Suppose $f^n \in \left(x^2+1\right)$. Since x^2+1 is irreducible and $x^2+1 \mid f^n$, we must have $x^2+1 \mid f$, hence $f \in \left(x^2+1\right)$, so $\sqrt{(x^2+1)} = \left(x^2+1\right)$. Over $\mathbb{C}[x]$, we claim that $\left(x^2+1\right)$ is neither prime nor maximal, but still radical. It is not prime as $x^2+1 = (x+i)(x-i)$ and hence also not maximal since $\left(x^2+1\right) \subset (x+i) \neq \mathbb{C}[x]$, where inequality follows from $(x+i)$ only having polynomials of degree ≥ 1.
Now suppose $f^n \in \left(x^2+1\right)$. Then $x+i, x-i \mid f^n$, hence both must divide f as they are irreducible, so $x^2+1 \mid f$. Thus $f \in \left(x^2+1\right)$, so $\sqrt{(x^2+1)} = \left(x^2+1\right)$ over $\mathbb{C}[x]$ as well.

(ii) Since $\left(x^2+1\right)$ is a prime ideal in $\mathbb{R}[x]$ by the previous exercise, we find by Eisenstein's criterion that y^2+x^2+1 is irreducible in $\mathbb{R}[x][y] =: \mathbb{R}[x,y]$.

(iii)
Let $C = \left\{f \in C\left(\mathbb{R}^2, \mathbb{R}\right) \mid \forall x \in \mathbb{R}\colon f(x,0) = 0\right\} \subset C\left(\mathbb{R}^2, \mathbb{R}\right)$. We claim that C is radical, but neither prime nor maximal.
To see that it is radical, suppose $g^n \in C$, so $g(x,0) \cdot \ldots \cdot g(x,0) = g^n(x,0) = 0$. Since $\mathbb{R}$ is an integral domain, this forces $g(x,0) = 0$, so $g \in C$. Thus $\sqrt{C} = C$.
Now let $h(x) = \mathbb{1}_{\geq 0}(x)x$ and $k(x) = \mathbb{1}_{\leq 0}(x)x$. Then $h, k \notin C$, but $hk \in C$. Therefore, C is not prime. Since $C\left(\mathbb{R}^2, \mathbb{R}\right)$ is a commutative ring and maximal ideals are prime over a commutative ring, we thus also conclude that C is not maximal.

(iv) The ideal (5) in $\mathbb{Z}[i]$ is not prime, hence not maximal as $\mathbb{Z}[i]$ is commutative. It is not prime because $5 = (2+i)(2-i)$.
For the radical part, if $a+bi \in \sqrt{(5)}$, then $(2+i)(2-i) \mid (a+bi)^n$, so $2+i \mid a+bi$ and $2-i \mid a+bi$ since each is irreducible, hence $5 \mid a+bi$, so $\sqrt{(5)} = (5)$.

(v) We claim that $(n) \subset \mathbb{Z}$ is prime and maximal whenever n is a prime and not otherwise. If n is not prime, then writing $n = ab$ for $a, b > 1$, we have $(n) = (a)(b)$, so (n) is not prime, hence not maximal as $\mathbb{Z}$ is commutative so all maximal ideals are prime ideals. If instead n is a prime, $n = p$, then (p) is both maximal and prime since $\mathbb{Z}/p$ is a field.
Suppose now $m \in \sqrt{(n)}$. Then $m^k \in (n)$, so $m^k = nq$ for some $q \in \mathbb{Z}$. Suppose n is squarefree. Let $p \mid n$. Then $p \mid m^k$ and thus $p \mid m$, so $n \mid m$, hence $m \in (n)$.

Conversely, if n is not squarefree, then letting $n = p^k q$ for some $k > 1$, we have $p^{k-1}q \in \sqrt{(n)}$ while $p^{k-1}q \notin (n)$, so (n) is not radical. □

Exercise 0.2 (2)**.** Let $n \in \mathbb{N}$. We denote the set of orthogonal matrices on $\mathbb{R}^n$ by

$$O(\mathbb{R}^n) = \left\{A \in \mathbb{R}^{n\times n} \mid A^T A = I_n\right\}$$

Write $R = \mathbb{R}[x_{ij} \mid i,j = 1,\dots,n]$ for the polynomial ring in variables $X = (x_{ij})_{i,j=1,\dots,n}$.

(1) Show that $O(\mathbb{R}^n)$ is the zero set $\mathbb{V}(I)$ of the ideal $I = (\{f_{ij} \mid i,j = 1,\dots,n\})$ of R where

$$f_{i,j} = \sum_{k=1}^n x_{ki}x_{kj} \quad \text{for } i \neq j \quad \text{and} \quad f_{ii} = \sum_{k=1}^n x_{ki}^2 - 1.$$

(2) Show that $O(\mathbb{R}^n)$ is also the real zero set of the ideal $J = (g,h)$ generated by the polynomials $g = \det(X)^2 - 1$ and $h = \sum_{i,j=1}^n x_{ij}^2 - n$.

Proof. (a) We know that $A = (\alpha_{ij}) \in O(\mathbb{R}^n)$ if and only if $A^T A = I$. Taking entries of either side of this equality, we get that A is orthogonal if and only if both of the following conditions hold:

$$0 = \left(A^T A\right)_{ij} = \sum_{k=1}^n \left(A^T\right)_{ik} A_{kj} = \sum_{k=1}^n \alpha_{ki}\alpha_{kj}$$
$$1 = \left(A^T A\right)_{ii} = \sum_{k=1}^n \alpha_{ki}^2.$$

That is, $A \in O(\mathbb{R}^n)$ if and only if $A \in \mathbb{V}(I)$ where we identify $R \cong M_n(\mathbb{R})$ by $\sum \alpha_{ij}x_{ij} \mapsto (\alpha_{ij})$.

(b) Firstly, suppose $A \in O(\mathbb{R}^n)$. Then $A^T A = I$. Therefore, $\det(A)^2 - 1 = \det(A^T)\det(A) - 1 = \det(A^T A) - 1 = \det(I) - 1 = 0$, so $g(A) = 0$. And now

$$n = \operatorname{tr}(I) = \operatorname{tr}(A^T A) = \sum_{k=1}^n \left(A^T A\right)_{kk} = \sum_{k,r=1}^n \alpha_{rk}^2$$

hence also $h(A) = 0$. Therefore $O(\mathbb{R}^n) \subset \mathbb{V}(J)$.
Conversely, suppose $A = (\alpha_{ij}) \in \mathbb{V}(J)$. Firstly, note that since

$$x^T A^T A x = (Ax)^T Ax = \|Ax\|^2 \geq 0,$$

the matrix $A^T A$ is positive semi-definite, hence all its eigenvalues are non-negative real numbers. In particular, $\sqrt[n]{\Pi_{i=1}^n \lambda_i}$ is well-defined where $\lambda_1,\dots,\lambda_m$ are the eigenvalues of $A^T A$ listed with repetition, and we can apply the AMGM inequality. Recall that the AMGM inequality tells us that

$$\frac{\sum_i \lambda_i}{n} \geq \sqrt[n]{\prod_i \lambda_i}$$

with equality if and only if all the λ_i are equal. But by Jordan normal form, $\operatorname{tr}\left(A^T A\right) = \sum_i \lambda_i$, and $\det\left(A^T A\right) = \prod_i \lambda_i$, so we obtain

$$\operatorname{tr}(A^T A) \geq n \det\left(A^T A\right)$$

with equality if and only if all eigenvalues are equal. But since $A \in \mathbb{V}(J)$, we have $g(A) = 0$, so $\det\left(A^T A\right) = \det(A)^2 = 1$. Likewise,

$$\operatorname{tr}\left(A^T A\right) = \sum_{k=1}^{n} \left(A^T A\right)_{kk} = \sum_{k,r=1}^{n} \alpha_{rk}^2 = h(A) + n = n$$

Thus we get

$$n = \operatorname{tr}\left(A^T A\right) \geq n \det\left(A^T A\right) = n$$

so we conclude that, since we have equality between the two sides, all eigenvalues of $A^T A$ must be equal. Now since $A^T A$ is self-adjoint, it is in particular diagonable, hence it has precisely n eigenvalues counted with multiplicity. Therefore, it has one eigenvalue with multiplicity n. Letting wlog λ denote this eigenvalue, we get

$$n\lambda = \operatorname{tr}\left(A^T A\right) = n$$

so $\lambda = 1$ since $\mathbb{R}$ is an integral domain. To see that this forces $A^T A$ to be I, we note that since $A^T A$ is diagonable, we can find some invertible linear map $P \in \mathrm{GL}_n(\mathbb{R})$ such that $PA^T AP^{-1} = I$, implying $A^T A = I$. Thus A is orthogonal, so $A \in O(\mathbb{R}^n)$. This gives the inclusion $\mathbb{V}(J) \subset O(\mathbb{R}^n)$. $\square$