Modern Algebra II
Fall 2019

Assignment 4.3
Due October 2

Exercise 1. Let R be a ring and P_1, P_2 prime ideals in R, neither containing the other. Explain why $P_1 \cap P_2$ need not be prime. Provide an example in which this is the case.

Exercise 2. An ideal A in a ring R is called *radical* if for all $a \in R$ and $n \in \mathbb{N}$, $a^n \in A$ implies $a \in A$. Note that every prime ideal is necessarily radical.

- **a.** Classify the radical ideals in $\mathbb{Z}$. Use your classification to give an example of a non-prime radical ideal. This shows that being prime is stronger than being radical.
- **b.** Prove that A is radical if and only if $\sqrt{A} = A$. Conclude that, when R is commutative, $\sqrt{A}$ is a radical ideal. See Exercise 3.1.2.
- **c.** Let $\mathcal{P}$ be a collection of prime ideals in R. Prove that when R is commutative, $\bigcap_{P \in \mathcal{P}} P$ is a radical ideal.

Exercise 3. Prove that if $M_1 \neq M_2$ are distinct maximal ideals in a ring R, then $M_1 + M_2 = R$. Conclude that if R is commutative, then $R/M_1M_2 \cong R/M_1 \times R/M_2$.

Exercise 4. Let $E_i : \mathbb{Z}[X] \to \mathbb{C}$ denote the evaluation at $i = \sqrt{-1}$ homomorphism. Use E_i to show that $\mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i]$. Conclude that the ideal (X^2+1) is prime in $\mathbb{Z}[X]$, but not maximal.

Exercise 5. If p is a prime number with $p \equiv 1 \,(\text{mod } 4)$, the theory of quadratic residues implies that there is an $n \in \mathbb{Z}$ so that $n^2 \equiv -1 \pmod{p}$. Choose such an n.

- **a.** Prove that in $\mathbb{Z}[X]$ we have $(X^2+1, p) = (X^2 - n^2, p) = \underbrace{(X-n, p)(X+n, p)}_{A}$. Deduce that (X^2+1, p) is a radical ideal. See Exercises 2c and 3.
- **b.** Use the Chisese remainder theorem to conclude that

$$\mathbb{Z}[X]/(X^2+1, p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},$$

and use this to determine whether (X^2+1, p) is prime, maximal or neither.

Remarks.

1. Exercises 1 and 2 tell us that although intersections of prime ideals aren't necessarily prime, they do still have the (weaker) property of being radical. Radical ideals figure prominently in classical algebraic geometry.

2. In Exercise 2, the radical $\sqrt{A}$ is defined *as a set* whether or not R is commutative. Commutativity is needed in part **b** only to guarantee that $\sqrt{A}$ is actually an *ideal* (recall that proving this requires the binomial theorem).

3. The use of the commutativity hypothesis is equally subtle in part **c** of Exercise 2. Let's say that an ideal P satisfying $ab \in P \;\Rightarrow\; a \in P$ or $b \in P$ is *EW-prime* (EW is for *element-wise*). To prove the intersection in part **c** is radical, you'll want to take advantage of EW-primality. But prime ideals are guaranteed to be EW-prime only if we assume R is commutative. In other words, R needs to be commutative just so that EW-prime is equivalent to prime.

4. Because every proper ideal A in a ring R is contained in a maximal ideal, the collection $Z(A) = \{P \subset R \,|\, P \text{ is prime and } A \subset P\}$ is nonempty. Therefore, when R is commutative, the ideal $\bigcap_{P \in Z(A)} P$ in Exercise 2c is a radical ideal containing A. We will prove that, in fact, this intersection is precisely $\sqrt{A}$.

5. Exercise 3 generalizes to any finite collection of maximal ideals in R.

6. To show that $p \in A$ in Exercise 5, first show that $2np \in A$. Then apply Bézout's lemma to $2n$ and p, and multiply the result by p.

7. For *any* p, the ideal $(X^2 + 1, p)$ in $\mathbb{Z}[X]$ is the kernel of the composite map

   $$\mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X] \to (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1).$$

   This can be used to recover the results of Exercise 5, and to show that, when $p \equiv -1 \pmod 4$, $(X^2 + 1, p)$ is a maximal ideal whose quotient ring is a field with p^2 elements. The prime $p = 2$ can also be handled this way, but the results appear somewhat mysterious: $(X^2 + 1, 2) = (X + 1, 2)^2$ with quotient ring isomorphic to the subring

   $$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z}/2\mathbb{Z} \right\}$$

   of $M_2(\mathbb{Z}/2\mathbb{Z})$. However, the details of this argument require a more thorough discussion of polynomial rings.