THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Homework 9
Due Date: 30th November 2023

Compulsory Part

1. Let R be a commutative ring and I an ideal of R. Show that the set $\sqrt{I}$ of all $a \in R$, such that $a^n \in I$ for some $n \in \mathbb{Z}^+$, is an ideal of R, called the **radical** of I.

   Proof. Clearly, $0^1 = 0 \in I$, so $0 \in \sqrt{I}$.

   Let $x, y \in \sqrt{I}$. Then $x^m, y^n \in I$ for some $m, n > 0$. Then $(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}$. But for any $0 \leq k \leq m+n$, either $k \geq m$ or $m+n-k \geq n$. Hence either $x^k \in I$ or $y^{m+n-k} \in I$. It follows that each summand and hence $(x+y)^{m+n}$ is in I. Then $x+y \in \sqrt{I}$.

   Let $a \in R, x \in \sqrt{I}$ Then $x^m \in I$ for some $m > 0$. Then $(ax)^m = a^m x^m \in I$. Therefore, $ax \in \sqrt{I}$.

   It follows that $\sqrt{I}$ is an ideal. □

2. Show by examples that for proper ideals I of a commutative ring R,

   (a) $\sqrt{I}$ need not equal I.
   (b) $\sqrt{I}$ may equal I.

   Proof. (a) Take $R = \mathbb{Z}[x]/\langle x^2 \rangle$ and $I = 0$. Then $x \in \sqrt{I} - I$ because $x^2 \in \langle x^2 \rangle$.

   (b) Take $R = \mathbb{Z}$ and $I = 0$. Then $\sqrt{I} = I$ because $\mathbb{Z}$ is an integral domain.

   □

3. Prove that $\mathbb{Z}[x]$ is not a PID by showing that the ideal $\langle 2, x \rangle$ is not principal.

   Proof. Suppose the ideal $\langle 2, x \rangle$ is principal ideal $\langle p(x) \rangle$. Since $2 \in \langle p(x) \rangle$, $2 = p(x)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Since $\mathbb{Z}$ is an integral domain, we have $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$. Thus, both $p(x)$ and $q(x)$ must be constant. The only possible options for $p(x)$ are $\{\pm 1, \pm 2\}$. However, This ideals obviously either contain units or not contain x. □

4. Let D be an integral domain. Show that, for $k = 1, \ldots, n$, the ideal $\langle x_1, \ldots, x_k \rangle$ is prime in $D[x_1, \ldots, x_n]$.

   Proof. Note that we have the isomorphism: $D[x_1, .., x_n]/\langle x_1, ..., x_k \rangle \simeq D[x_{k+1}, ..., x_n]$. We conclude that $\langle x_1, ..., x_n \rangle$ is a prime ideal since $D[x_{k+1}, ..., x_n]$ is an integral domain.

   □

5. Let $\varphi : R \to S$ be a homomorphism of commutative rings, and let $I \subset S$ be an ideal. Prove that if I is a prime ideal in S, then $\varphi^{-1}(I)$ is a prime ideal in R. Show by giving an exmple that, however, $\varphi^{-1}(I)$ is not necessarily maximal when I is maximal.

   Proof. Let $\varphi : R \to S$ be a homomorphism of commutative rings, and let $I \subset S$ be an ideal. Suppose I is prime in S. Let $x, y \in R$ with $xy \in \varphi^{-1}(I)$. Then $\varphi(x)\varphi(y) = \varphi(xy) \in I$. Since I is prime, $\varphi(x) \in I$ or $\varphi(y) \in I$. Therefore, $x \in \varphi^{-1}(I)$ or $y \in \varphi^{-1}(I)$. It follows that $\varphi^{-1}(I)$ is a prime ideal in R.

   Consider the embedding $\mathbb{Z} \to \mathbb{Q}$, $\{0\}$ is a maximal ideal in $\mathbb{Q}$, but its preimage $\{0\}$ is not a maximal ideal in $\mathbb{Z}$. □

6. Let R be a commutative ring, and let P be a prime ideal of R. Suppose that 0 is the only zero-divisor of R contained in P. Show that R is an integral domain.

   Proof. Let $x, y \in R$. Suppose $xy = 0$. Then $xy \in P$, and so $x \in P$ or $y \in P$. Without loss of generality, we assume that $x \in P$. If $y \neq 0$, then x is a zero-divisor of R contained in P. Then $x = 0$. It follows that $y = 0$ or $x = 0$. Therefore, R is an integral domain. □

7. Show that every prime ideal in a *finite* commutative ring R is a maximal ideal.

   Proof. Let R be a finite commutative ring. Let P be a prime ideal in R. Then R/P is a finite integral domain. Let $x \in R/P$ be a nonzero element. Let $m_x : R/P \to R/P$ be defined by $m_x(y) = xy$. If $m_x(y) = m_x(y')$, then $x(y - y') = m_x(y - y') = 0$. Then $y - y' = 0$ since R/P is an integral domain. Therefore, m_x is injective. Since R/P is finite, m_x is surjective. Therefore, $xy = m_x(y) = 1$ for some $y \in R/P$. Then x is a unit in R/P. It follows that R/P is a field. Therefore, P is a maximal ideal in R. □

Optional Part

1. An element a of a ring R is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$.
   Show that the collection N of all nilpotent elements in a commutative ring R is an ideal, called the **nilradical** of R.

   Proof. Note that it is just the set $\sqrt{\{0\}}$. By Ex.1 in the compulsory part, it is an ideal. □

2. Show that the nilradical N of a commutative ring R is contained in every prime ideal of R.

   Proof. By definition of prime ideals, $x^k = 0 \in P \Rightarrow x \in P$ for any prime ideal P. Thus the nilradical is contained in each prime ideal. □

3. What is the relationship between the radical $\sqrt{I}$ of an ideal I in a commutative ring R and the nilradical of the quotient ring R/I? Explain your answer carefully.

   Proof. Let $\pi : R \to R/I$ be the natural projection. Then $\pi(\sqrt{I}) = \sqrt{0_{R/I}}$. We give a proof: For any $x \in \sqrt{I}, x^n \in I$ for some $n > 0$. Then $\pi(x)^n \in 0_{R/I}$, and so $\pi(x) \in \sqrt{0_{R/I}}$. Therefore, $\pi(\sqrt{I}) \subseteq \sqrt{0_{R/I}}$.
   Conversely, let $y \in \sqrt{0_{R/I}}$, then $y^n = 0_{R/I}$ for some $n > 0$. Since π is surjective, $\pi(x) = y$ for some $x \in R$. Then $\pi(x^n) = y^n = 0_{R/I}$. Then $x^n \in I$, and so $x \in \sqrt{I}$. Then $y = \pi(x) \in \pi(\sqrt{I})$. It follows that $\pi(\sqrt{I}) = \sqrt{0_{R/I}}$.
   Since $\sqrt{I} \supseteq I = \ker(\pi)$, $\sqrt{I}$ is the ideal corresponding to $\sqrt{0_{R/I}}$ via π.

   □

4. Let F be a subfield of a field E.

   (a) For $\alpha_1, \ldots, \alpha_n \in E$, define the *evaluation map*

   $$\phi_{\alpha_1,\cdots,\alpha_n} : F[x_1, \cdots, x_n] \to E$$

   by sending $f(x_1, \ldots, x_n)$ to $f(\alpha_1, \ldots, \alpha_n)$. Show that $\phi_{\alpha_1,\cdots,\alpha_n}$ is a ring homomorphism. We say that $(\alpha_1, \cdots, \alpha_n) \in F^n$ is a zero of $f = f(x_1, \cdots, x_n)$ if $f(\alpha_1, \ldots, \alpha_n) = 0$, or equivalently, if $\phi_{\alpha_1,\cdots,\alpha_n}(f) = 0$.

   (b) Given a subset $V \subset F^n$, show that the set of polynomials $f \in F[x_1, \cdots, x_n]$ such that every element in V is a zero of f forms an ideal of $F[x_1, \cdots, x_n]$.

   Proof. (a) It is the multi-variable evaluation homomorphism, and can be realized as $(ev_{\alpha_1} \circ ev_{\alpha_2} \circ ... \circ ev_{\alpha_n})|_{F[x_1,\cdots,x_n]}$, where each $ev_{\alpha_r} : E[x_1, ..., x_r] = E[x_1, ..., x_{r-1}][x_r] \to E[x_1, ..., x_{r-1}]$ is the evaluation homomorphism sending x_r to α_r.

   (b) That set is $\bigcap_{(\alpha_1,\cdots,\alpha_n)\in V} \ker(\phi_{\alpha_1,\cdots,\alpha_n})$, and is an ideal of $F[x_1, ..., x_n]$

   □

5. Prove the *equivalence* of the following two statements:
   Fundamental Theorem of Algebra: Every nonconstant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$.
   Nullstellensatz for $\mathbb{C}[x]$: Let $f_1(x), \ldots, f_r(x) \in \mathbb{C}[x]$ and suppose that every $\alpha \in \mathbb{C}$ that is a zero of all r of these polynomials is also a zero of a polynomial $g(x)$ in $\mathbb{C}[x]$. Then some power of $g(x)$ is in the smallest ideal of $\mathbb{C}[x]$ that contains the r polynomials $f_1(x), \ldots, f_r(x)$.

   Proof. $(FTA \implies N)$ Suppose we have FTA. Then every nonconstant polynomial in $\mathbb{C}[x]$ factors into $c(x-z_1)^{k_1}...(x-z_r)^{k_r}$ for some $c, z_1, ..., z_r \in \mathbb{C}, k_1, ..., k_r \in \mathbb{Z}_{>0}$.

   Let $f_1(x), \ldots, f_r(x) \in \mathbb{C}[x]$ and suppose that every $\alpha \in \mathbb{C}$ that is a zero of all r of these polynomials is also a zero of a polynomial $g(x)$ in $\mathbb{C}[x]$. Let $I = (f_1, ..., f_r)$. Since $\mathbb{C}[x]$ is a PID, $I = (h)$ for some $h \in \mathbb{C}[x]$.

   Case 1. h is not a constant polynomial. Write $h = c(x-z_1)^{k_1}...(x-z_s)^{k_s}$ as above. Note that each $f_j \in (h)$, so $h|f_j$ for each j. Then each z_i is a root of h, hence a root of f_j for each j. By assumption $g(z_i) = 0$ for each $i = 1, 2, ..., s$. Then $(x-z_1)...(x-z_s) \mid g$. Then $g^{\max(k_1,...,k_s)} \in (h) = I$.

   Case 2. h is a constant. If $h \neq 0$, then $(h) = (1)$, and $g \in (h)$. If $h = 0$, then each $f_i = 0$, so g is zero everywhere on $\mathbb{C}$, and so $g = 0 \in (h)$.

   $(FTA \impliedby N)$ Conversely, suppose we have N. Let f be a nonconstant polynomial in $\mathbb{C}[x]$. Suppose f has no root in $\mathbb{C}$. Let $g = 1$, then any root of f is a root of g, and by N, $g^n \in (f)$. But then $1 \in (f)$. This is absurd because $\deg(f) > 0$. Therefore, f has a root in $\mathbb{C}$. □