Example. Consider $\mathbf{Z} \to \mathbf{Z}[i]$, where $i = \sqrt{-1}$. A prime ideal (p) of $\mathbf{Z}$ may or may not stay prime when extended to $\mathbf{Z}[i]$. In fact $\mathbf{Z}[i]$ is a principal ideal domain (because it has a Euclidean algorithm) and the situation is as follows:

i) $(2)^e = ((1+i)^2)$, the *square* of a prime ideal in $\mathbf{Z}[i]$;

ii) If $p \equiv 1 \pmod 4$ then $(p)^e$ is the product of two distinct prime ideals (for example, $(5)^e = (2+i)(2-i)$);

iii) If $p \equiv 3 \pmod 4$ then $(p)^e$ is prime in $\mathbf{Z}[i]$.

Of these, ii) is not a trivial result. It is effectively equivalent to a theorem of Fermat which says that a prime $p \equiv 1 \pmod 4$ can be expressed, essentially uniquely, as a sum of two integer squares (thus $5 = 2^2 + 1^2$, $97 = 9^2 + 4^2$, etc.).

In fact the behavior of prime ideals under extensions of this sort is one of the central problems of algebraic number theory.

Let $f: A \to B$, $\mathfrak{a}$ and $\mathfrak{b}$ be as before. Then

Proposition 1.17. i) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$;

ii) $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$;

iii) *If C is the set of contracted ideals in A and if E is the set of extended ideals in B, then $C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, $E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$, and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijective map of C onto E, whose inverse is $\mathfrak{b} \to \mathfrak{b}^c$.*

Proof. i) is trivial, and ii) follows from i).

iii) If $\mathfrak{a} \in C$, then $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec}$; conversely if $\mathfrak{a} = \mathfrak{a}^{ec}$ then $\mathfrak{a}$ is the contraction of $\mathfrak{a}^e$. Similarly for E. ■

Exercise 1.18. *If $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of A and if $\mathfrak{b}_1, \mathfrak{b}_2$ are ideals of B, then*

$$
\begin{array}{ll}
(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e, & (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\
(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\
(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e, & (\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c, \\
(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e), & (\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\
r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e), & r(\mathfrak{b})^c = r(\mathfrak{b}^c).
\end{array}
$$

The set of ideals E is closed under sum and product, and C is closed under the other three operations.

"ring" means commutative ring with 1

EXERCISES

1. Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

2. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that

i) f is a unit in $A[x] \Leftrightarrow a_0$ is a unit in A and $a_1, \ldots, a_n$ are nilpotent. [If $b_0 + b_1x + \cdots + b_mx^m$ is the inverse of f, prove by induction on r that $a_n^{r+1}b_{m-r} = 0$. Hence show that a_n is nilpotent, and then use Ex. 1.]

ii) f is nilpotent $\Leftrightarrow a_0, a_1, \ldots, a_n$ are nilpotent.

iii) f is a zero-divisor $\Leftrightarrow$ there exists $a \neq 0$ in A such that $af = 0$. [Choose a polynomial $g = b_0 + b_1x + \cdots + b_mx^m$ of least degree m such that $fg = 0$. Then $a_nb_m = 0$, hence $a_ng = 0$ (because a_ng annihilates f and has degree $< m$). Now show by induction that $a_{n-r}g = 0$ $(0 \leqslant r \leqslant n)$.]

iv) f is said to be *primitive* if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

3. Generalize the results of Exercise 2 to a polynomial ring $A[x_1, \ldots, x_r]$ in several indeterminates.

4. In the ring $A[x]$, the Jacobson radical is equal to the nilradical.

5. Let A be a ring and let $A[[x]]$ be the ring of formal power series $f = \sum_{n=0}^{\infty} a_nx^n$ with coefficients in A. Show that

i) f is a unit in $A[[x]] \Leftrightarrow a_0$ is a unit in A.

ii) If f is nilpotent, then a_n is nilpotent for all $n \geqslant 0$. Is the converse true? (See Chapter 7, Exercise 2.)

iii) f belongs to the Jacobson radical of $A[[x]] \Leftrightarrow a_0$ belongs to the Jacobson radical of A.

iv) The contraction of a maximal ideal $\mathfrak{m}$ of $A[[x]]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x.

v) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

6. A ring A is such that every ideal not contained in the nilradical contains a non-zero idempotent (that is, an element e such that $e^2 = e \neq 0$). Prove that the nilradical and Jacobson radical of A are equal.

7. Let A be a ring in which every element x satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in A is maximal.

8. Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

9. Let $\mathfrak{a}$ be an ideal $\neq (1)$ in a ring A. Show that $\mathfrak{a} = r(\mathfrak{a}) \Leftrightarrow \mathfrak{a}$ is an intersection of prime ideals.

10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following are equivalent:

i) A has exactly one prime ideal;

ii) every element of A is either a unit or nilpotent;

iii) $A/\mathfrak{N}$ is a field.

11. A ring A is *Boolean* if $x^2 = x$ for all $x \in A$. In a Boolean ring A, show that

i) $2x = 0$ for all $x \in A$;

ii) every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p}$ is a field with two elements;

iii) every finitely generated ideal in A is principal.

12. A local ring contains no idempotent $\neq 0, 1$.

Construction of an algebraic closure of a field (E. Artin).

13. Let K be a field and let Σ be the set of all irreducible monic polynomials f in one

polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$, where $\sigma_1, \ldots, \sigma_n$ are in K. But K is algebraic over F; therefore, by several uses of Theorem 5.1.3, $M = F(\sigma_1, \ldots, \sigma_n)$ is a finite extension of F. Since u satisfies the polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ whose coefficients are in M, u is algebraic over M. Invoking Theorem 5.1.2 yields that $M(u)$ is a finite extension of M. However, by Theorem 5.1.1, $[M(u):F] = [M(u):M][M:F]$, whence $M(u)$ is a finite extension of F. But this implies that u is algebraic over F, completing proof of the theorem.

A quick description of Theorem 5.1.5: algebraic over algebraic is algebraic.

The preceding results are of special interest in the particular case in which F is the field of rational numbers and K the field of complex numbers.

DEFINITION A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

A complex number which is not algebraic is called *transcendental*. At the present stage we have no reason to suppose that there are any transcendental numbers. In the next section we shall prove that the familiar real number e is transcendental. This will, of course, establish the existence of transcendental numbers. In actual fact, they exist in great abundance; in a very well-defined way there are more of them than there are algebraic numbers.

Theorem 5.1.4 applied to algebraic numbers proves the interesting fact that *the algebraic numbers form a field*; that is, the sum, products, and quotients of algebraic numbers are again algebraic numbers.

Theorem 5.1.5 when used in conjunction with the so-called "fundamental theorem of algebra," has the implication that the roots of a polynomial whose coefficients are algebraic numbers are themselves algebraic numbers.

Problems

1. Prove that the mapping $\psi: F[x] \to F(a)$ defined by $h(x)\psi = h(a)$ is a homomorphism.
2. Let F be a field and let $F[x]$ be the ring of polynomials in x over F. Let $g(x)$, of degree n, be in $F[x]$ and let $V = (g(x))$ be the ideal generated by $g(x)$ in $F[x]$. Prove that $F[x]/V$ is an n-dimensional vector space over F.
3. (a) If V is a finite-dimensional vector space over the field K, and if F is a subfield of K such that $[K:F]$ is finite, show that V is a finite-dimensional vector space over F and that moreover $\dim_F(V) = (\dim_K(V))([K:F])$.
   (b) Show that Theorem 5.1.1 is a special case of the result of part (a).

4. (a) Let R be the field of real numbers and Q the field of rational numbers. In R, $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over Q. Exhibit a polynomial of degree 4 over Q satisfied by $\sqrt{2} + \sqrt{3}$.
   (b) What is the degree of $\sqrt{2} + \sqrt{3}$ over Q? Prove your answer.
   (c) What is the degree of $\sqrt{2}\,\sqrt{3}$ over Q?

5. With the same notation as in Problem 4, show that $\sqrt{2} + \sqrt[3]{5}$ is algebraic over Q of degree 6.

*6. (a) Find an element $u \in R$ such that $Q(\sqrt{2}, \sqrt[3]{5}) = Q(u)$.
   (b) In $Q(\sqrt{2}, \sqrt[3]{5})$ characterize all the elements w such that $Q(w) \neq Q(\sqrt{2}, \sqrt[3]{5})$.

7. (a) Prove that $F(a, b) = F(b, a)$.
   (b) If $(i_1, i_2, \ldots, i_n)$ is any permutation of $(1, 2, \ldots, n)$, prove that

$$F(a_1, \ldots, a_n) = F(a_{i_1}, a_{i_2}, \ldots, a_{i_n}).$$

8. If $a, b \in K$ are algebraic over F of degrees m and n, respectively, and if m and n are relatively prime, prove that $F(a, b)$ is of degree mn over F.

9. Suppose that F is a field having a finite number of elements, q.
   (a) Prove that there is a prime number p such that $\underbrace{a + a + \cdots + a}_{p\text{-times}} = 0$ for all $a \in F$.
   (b) Prove that $q = p^n$ for some integer n.
   (c) If $a \in F$, prove that $a^q = a$.
   (d) If $b \in K$ is algebraic over F, prove $b^{q^m} = b$ for some $m > 0$.

An algebraic number a is said to be an *algebraic integer* if it satisfies an equation of the form $a^m + \alpha_1 a^{m-1} + \cdots + \alpha_m = 0$, where $\alpha_1, \ldots, \alpha_m$ are integers.

10. If a is any algebraic number, prove that there is a positive integer n such that na is an algebraic integer.

11. If the rational number r is also an algebraic integer, prove that r must be an ordinary integer.

12. If a is an algebraic integer and m is an ordinary integer, prove
   (a) $a + m$ is an algebraic integer.
   (b) ma is an algebraic integer.

13. If α is an algebraic integer satisfying $\alpha^3 + \alpha + 1 = 0$ and β is an algebraic integer satisfying $\beta^2 + \beta - 3 = 0$, prove that both $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.

**14. (a) Prove that the sum of two algebraic integers is an algebraic integer.