4. Commutative rings I

Throughout this section the rings in question will be commutative, and will have a unit 1.

---

1. *Divisibility and ideals*

Many of the primitive ideas about divisibility we bring from the ordinary integers $\mathbb{Z}$, though few of the conclusions are as simple in any generality.

Let R be a commutative [1] ring with unit [2] 1. Let $\mathbb{R}^\times$ be the group of units in R.

Say d **divides** m, equivalently, that m is a **multiple** of d, if there exists a $q \in R$ such that $m = qd$. Write $d|m$ if d divides m. It is easy to prove, from the definition, that if $d|x$ and $d|y$ then $d|(ax + by)$ for any $x, y, a, b \in R$: let $x = rd$ and $y = sd$, and

$$ax + by = a(rd) + b(sd) = d \cdot (ar + bs)$$

A ring element d is a **common divisor** of ring elements $n_1, \ldots, n_m$ if d divides each n_i. A ring element N is a **common multiple** of ring elements $n_1, \ldots, n_m$ if N is a multiple of each.

[1] Divisibility and ideals can certainly be discussed without the assumption of commutativity, but the peripheral complications obscure simpler issues.

[2] And, certainly, one can contemplate divisibility in rings without units, but this leads to needlessly counterintuitive situations.

A divisor d of n is **proper** if it is not a unit multiple of n and is not a unit itself. A ring element is **irreducible** if it has no proper factors. A ring element p is **prime** if $p|ab$ implies $p|a$ or $p|b$ and p is not a unit and is not 0. [3] If two prime elements p and p' are related by $p = up'$ with a unit u, say that p and p' are **associate**. We view associate primes as being essentially identical. [4] Recall that an **integral domain** [5] is a commutative ring in which $cd = 0$ implies either c or d is 0. [6]

[1.0.1] **Proposition:** Prime elements of an integral domain R are irreducible. [7]

Proof: Let p be a prime element of R, and suppose that $p = ab$. Then $p|ab$, so $p|a$ or $p|b$. Suppose $a = a'p$. Then $p = p \cdot a'b$, and $p \cdot (1 - a'b) = 0$. Since the ring is an integral domain, either $p = 0$ or $a'b = 1$, but $p \neq 0$. Thus, $a'b = 1$, and b is a unit. This proves that any factorization of the prime p is non-proper. ///

An integral domain R with 1 is a **unique factorization domain** (**UFD**) if every element $r \in R$ has a unique (up to ordering of factors and changing primes by units) expression

$$r = up_1 \dots p_\ell$$

with unit u and primes p_i.

[1.0.2] **Remark:** The ordinary integers are the primary example of a UFD. The second important example is the ring of polynomials in one variable over a field, treated in the next section.

[3] Yes, the definition of *prime* rewrites what was a theorem for the ordinary integers as the definition in general, while demoting the lack of proper factors to a slightly more obscure classification, of *irreducibility*.

[4] In the case of the ordinary integers, $\pm p$ are associate, for prime p. We naturally distinguish the positive one of the two. But in more general situations there is not a reliable special choice among associates.

[5] Some sources have attempted to popularize the term *entire* for a ring with no proper zero divisors, but this has not caught on.

[6] If one insisted, one could say that an integral domain is a commutative ring in which 0 is prime, but for practical reasons we want our convention not to include 0 when we speak of prime *elements*. Likewise by convention we do not want *units* to be included when we speak of primes.

[7] The converse is not generally true.

2. *Polynomials in one variable over a field*

We will prove that the ring $k[x]$ of polynomials in one variable with coefficients in a field k is *Euclidean*, and thus has unique factorization. This example is comparable in importance to $\mathbb{Z}$ and its elementary properties.

As usual, the **degree** of a polynomial $\sum_i c_i x^i$ is the highest index i such that $c_i \neq 0$.

[2.0.1] **Proposition:** For polynomials P, Q with coefficients in a field [8] k, the degree of the product is the sum of the degrees:

$$\deg(P \cdot Q) = \deg P + \deg Q$$

[2.0.2] **Remark:** To make this correct even when one of the two polynomials is the 0 polynomial, the 0 polynomial is by convention given degree $-\infty$.

Proof: The result is clear if either polynomial is the zero polynomial, so suppose that both are non-zero. Let

$$P(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_2 x^2 + a_1 x + a_0$$
$$Q(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_2 x^2 + b_1 x + b_0$$

where the (apparent) highest-degree coefficients a_m and b_n non-zero. Then in $P \cdot Q$ the highest-degree term is $a_m b_n x^{m+n}$. Since the product of non-zero elements of a field is non-zero, [9] the coefficient of x^{m+n} is non-zero. ///

[2.0.3] **Corollary:** *(Cancellation property)* For polynomials in $k[x]$, with a field k, let $A \cdot P = B \cdot P$ for a non-zero polynomial P. Then $A = B$.

Proof: The equality $AP = BP$ gives $(A - B)P = 0$. Because the degree of the product is the sum of the degrees of the factors,

$$\deg(A - B) + \deg P = \deg 0 = -\infty$$

Since P is non-zero, $\deg P \geq 0$. Then $\deg(A - B) = -\infty$, so $A - B = 0$, and $A = B$. ///

[2.0.4] **Corollary:** The group of units $k[x]^\times$ in the polynomial ring in one variable over a field k is just the group of units $k^\times$ in k. [10]

Proof: Suppose that $P \cdot Q = 1$. Then $\deg P + \deg Q = 0$, so both degrees are 0, that is, P and Q are in k. ///

A polynomial is **monic** if its highest degree coefficient is 1. Since elements of $k^\times$ are units in $k[x]$, any polynomial can be multiplied by a unit to make it monic.

[2.0.5] **Proposition:** (*Euclidean property*) Let k be a field and M a non-zero polynomial in $k[x]$. Let H be any other polynomial in $k[x]$. Then there are unique polynomials Q and R in $k[x]$ such that $\deg R < \deg M$ and

$$H = Q \cdot M + R$$

[8] The proof only uses the fact that a product of non-zero elements is necessarily non-zero. Thus, the same conclusion can be reached if the coefficients of the polynomials are merely in an *integral domain*.

[9] In case this is not clear: let a, b be elements of a field k with $ab = 0$ and $a \neq 0$. Since non-zero elements have inverses, there is a^{-1}, and $a^{-1}ab = a^{-1} \cdot 0 = 0$, but also $a^{-1}ab = b$. Thus, $b = 0$.

[10] We identify the scalars with degree-zero polynomials, as usual. If one is a bit worried about the legitimacy of this, the free-algebra definition of the polynomial ring can be invoked to prove this more formally.

Proof: [11] Let X be the set of polynomials expressible in the form $H - S \cdot M$ for some polynomial S. Let $R = H - Q \cdot M$ be an element of X of minimal degree. Claim that $\deg R < \deg M$. If not, let a be the highest-degree coefficient of R, let b be the highest-degree coefficient of M, and define

$$G = (ab^{-1}) \cdot x^{\deg R - \deg M}$$

Then

$$R - G \cdot M$$

removes the highest-degree term of R, and

$$\deg(R - G \cdot M) < \deg R$$

But $R - GM$ is still in X, since

$$R - G \cdot M = (H - Q \cdot M) - G \cdot M = H - (Q + G) \cdot M$$

By choice of R this is impossible, so, in fact, $\deg R < \deg M$. For uniqueness, suppose

$$H = Q \cdot M + R = Q' \cdot M + R'$$

Subtract to obtain

$$R - R' = (Q' - Q) \cdot M$$

Since the degree of a product is the sum of the degrees, and since the degrees of R, R' are less than the degree of M, this is impossible unless $Q' - Q = 0$, in which case $R - R' = 0$. ///

Compatibly with general terminology, a non-zero polynomial is **irreducible** if it has no proper divisors.

The **greatest common divisor** of two polynomials A, B is the *monic* polynomial g of highest degree dividing both A and B.

[2.0.6] **Theorem:** For polynomials f, g in $k[x]$, the monic polynomial of the form $sf + tg$ (for $s, t \in k[x]$) of smallest degree is the *gcd* of f, g. In particular, greatest common divisors exist.

Proof: Among the non-negative integer values $\deg(sf + tg)$ there is at least one which is minimal. Let $h = sf + tg$ be such, and multiply through by the inverse of the highest-degree coefficient to make h monic. First, show that $h|f$ and $h|g$. We have

$$f = q(sf + tg) + r$$

with $\deg r < \deg(sf + tg)$. Rearranging,

$$r = (1 - qs)f + (-qt)g$$

So r itself is $s'f + t'g$ with $s', t' \in k[x]$. Since $sf + tg$ had the smallest non-negative degree of any such expression, and $\deg r < \deg(sf + tg)$, it must be that $r = 0$. So $sf + tg$ divides f. Similarly, $sf + tg$ divides g, so $sf + tg$ is a divisor of both f and g. On the other hand, if $d|f$ and $d|g$, then certainly $d|sf + tg$.
///

[2.0.7] **Corollary:** Let P be an irreducible polynomial. For two other polynomials A, B, if $P|AB$ then $P|A$ or $P|B$. Generally, if an irreducible P divides a product $A_1 \dots A_n$ of polynomials then P must divide one of the factors A_i.

[11] This argument is identical to that for the ordinary integers, as are many of the other proofs here.

Proof: It suffices to prove that if $P|AB$ and $P \not| A$ then $P|B$. Since $P \not| A$, and since P is irreducible, the *gcd* of P and A is just 1. Therefore, there are $s, t \in k[x]$ so that

$$1 = sA + tP$$

Then

$$B = B \cdot 1 = B \cdot (sA + tP) = s(AB) + (Bt)P$$

Since $P|AB$, surely P divides the right-hand side. Therefore, $P|B$, as claimed.

[2.0.8] **Corollary:** Irreducible polynomials P in $k[x]$ are prime, in the sense that $P|AB$ implies $P|A$ or $P|B$ for polynomials A and B.

Proof: Let $AB = M \cdot P$, and suppose that P does not divide A. Since P is irreducible, any proper factor is a unit, hence a non-zero constant. Thus, $\gcd(P, A) = 1$, and there are polynomials R, S such that $RP + SA = 1$. Then

$$B = B \cdot 1 = B \cdot (RP + SA) = P \cdot BR + S \cdot AB = P \cdot BR + S \cdot M \cdot P = P \cdot (BR + SM)$$

so B is a multiple of P. ///

[2.0.9] **Corollary:** Any polynomial M in $k[x]$ has a unique factorization (up to ordering of factors) as

$$M = u \cdot P_1^{e_1} \dots P_\ell^{e_\ell}$$

where $u \in k^\times$ is a unit in $k[x]$, the P_i are distinct primes, and the exponents are positive integers.

Proof: [12] First prove existence by induction on degree. [13] Suppose some polynomial F admitted no such factorization. Then F is not irreducible (or the non-factorization is the factorization), so $R = A \cdot B$ with both of A, B of lower degree but not degree 0. By induction, both A and B have factorizations into primes.

Uniqueness is a sharper result, proven via the property that $P|AB$ implies $P|A$ or $P|B$ for prime P. As in the case of integers, given two alleged prime factorizations, any prime in one of them must be equal to a prime in the other, and by cancelling we do an induction to prove that all the primes are the same. ///

[2.0.10] **Proposition:** *(Testing for linear factors)* A polynomial $f(x)$ with coefficients in a field k has a linear factor $x - a$ (with $a \in k$) if and only if $F(a) = 0$.

Proof: If $x - a$ is a factor, clearly $f(a) = 0$. On the other hand, suppose that $f(a) = 0$. Use the division algorithm to write

$$f(x) = Q(x) \cdot (x - a) + R$$

Since $\deg R < \deg(x - a) = 1$, R is a constant. Evaluate both sides at a to obtain

$$0 = f(a) = Q(a) \cdot (a - a) + R = Q(a) \cdot 0 + R = R$$

Therefore, $R = 0$ and $x - a$ divides $f(x)$. ///

[12] It bears emphasizing that the argument here proves unique factorization from the propery of primes that $p|ab$ implies $p|a$ or $p|b$, which comes from the Euclidean property. There are many examples in which a unique factorization result does hold without Euclidean-ness, such as polynomial rings $k[x_1, \dots, x_n]$ in *several* variables over a field, but the argument is more difficult. See *Gauss' Lemma*.

[13] An induction on size completely analogous to the induction on size for the ordinary integers.

[2.0.11] **Corollary:** For polynomial P in $k[x]$, the equation $P(a) = 0$ has no more roots a than the degree of P.

Proof: By the proposition, a root gives a monic linear factor, and by unique factorization there cannot be more of these than the degree. ///

[2.0.12] **Example:** With coefficients not in a field, the intuition that a polynomial equation has no more roots than its degree is inaccurate. For example, with coefficients in $\mathbb{Z}/15$, the equation

$$a^2 - 1 = 0$$

has the obvious roots ± 1, but also the roots 6 and 10. And there are two different factorizations in $(\mathbb{Z}/15)[x]$

$$x^2 - 1 = (x-1)(x+1) = (x-6)(x-10)$$

---

3. *Ideals*

Let R be a commutative ring with unit 1. An **ideal** in R is an additive subgroup I of R such that $R \cdot I \subset I$. That is, I is an R-submodule of R with (left) multiplication.

[3.0.1] **Example:** One archetype is the following. In the ring $\mathbb{Z}$, for any fixed n, the set $n \cdot \mathbb{Z}$ of multiples of n is an ideal.

[3.0.2] **Example:** Let $R = k[x]$ be the ring of polynomials in one variable x with coefficients in a field k. Fix a polynomial $P(x)$, and let $I \subset R$ be the set of polynomial multiples $M(x) \cdot P(x)$ of $P(x)$.

[3.0.3] **Example:** Abstracting the previous two examples: fix $n \in R$. The set $I = n \cdot R = \{rn : r \in R\}$ of multiples of m is an ideal, the **principal ideal generated by** n. A convenient lighter notation is to write

$$\langle n \rangle = R \cdot n = \text{principal ideal generated by } n$$

[3.0.4] **Example:** In any ring, the **trivial ideal** is $I = \{0\}$. An ideal is **proper** if it is neither the trivial ideal $\{0\}$ nor the whole ring R (which is also an ideal).

[3.0.5] **Example:** If an ideal I contains a unit u in R, then $I = R$. Indeed, for any $r \in R$,

$$r = r \cdot 1 = r \cdot (u^{-1} \cdot u) \in r \cdot u^{-1} \cdot I \subset I$$

For two subsets X, Y of a *ring* R, write

$$X + Y = \{x + y : x \in X,\ y \in Y\}$$

and [14]

$$X \cdot Y = \{\text{finite sums } \sum_i x_i\, y_i : x_i \in X,\ y_i \in Y\}$$

In this notation, for an ideal I in a commutative ring R with 1 we have $R \cdot I = I$.

[14] Note that here the notation $X \cdot Y$ has a different meaning than it does in group theory, since in the present context it is implied that we take all finite sums of products, not just products.

An integral domain in which every ideal is principal is a **principal ideal domain**. [15]

[3.0.6] **Corollary:** [16] Every ideal I in $\mathbb{Z}$ is principal, that is, of the form $I = n \cdot \mathbb{Z}$. In particular, unless $I = \{0\}$, the integer n is the least positive element of I.

Proof: Suppose I is non-zero. Since I is closed under additive inverses, if I contains $x < 0$ then it also contains $-x > 0$. Let n be the least element of I. Let $x \in I$, take $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that

$$x = q \cdot n + r$$

Certainly qn is in I, and $-qn \in I$ also. Since $r = x - qn$, $r \in I$. Since n was the smallest positive element of I, $r = 0$. Thus, $x = qn \in n \cdot \mathbb{Z}$, as desired. ///

[3.0.7] **Corollary:** [17] Let k be a field. Let $R = k[x]$ be the ring of polynomials in one variable x with coefficients in k. Then every ideal I in R is principal, that is, is of the form $I = k[x] \cdot P(x)$ for some polynomial P. In particular, $P(x)$ is the monic polynomial of smallest degree in I, unless $I = \{0\}$, in which case $P(x) = 0$.

Proof: If $I = \{0\}$, then certainly $I = k[x] \cdot 0$, and we're done. So suppose I is non-zero. Suppose that $Q(x) = a_n x^n + \ldots + a_0$ lies in I with $a_n \neq 0$. Since k is a field, there is an inverse a_n^{-1}. Then, since I is an ideal, the polynomial

$$P(x) = a_n^{-1} \cdot Q(x) = x^n + a_n^{-1} a_{n-1} x^{n-1} + \ldots + a_n^{-1} a_0$$

also lies in I. That is, there is indeed a *monic* polynomial of lowest degree of any element of the ideal. Let $x \in I$, and use the Division Algorithm to get $Q, R \in k[x]$ with $\deg R < \deg P$ and

$$x = Q \cdot P + R$$

Certainly $Q \cdot P$ is still in I, and then $-Q \cdot P \in I$ also. Since $R = x - Q \cdot P$, we conclude that $R \in I$. Since P was the monic polynomial in I of smallest degree, it must be that $R = 0$. Thus, $x = Q \cdot P \in n \cdot k[x]$, as desired. ///

[3.0.8] **Remark:** The proofs of these two propositions can be abstracted to prove that every ideal in a Euclidean ring is principal.

[3.0.9] **Example:** Let R be a commutative ring with unit 1, and fix two elements $x, y \in R$. Then

$$I = R \cdot x + R \cdot y = \{rx + sy : r, s \in R\}$$

is an ideal in R. The two elements x, y are the **generators** of I.

[3.0.10] **Example:** Similarly, for fixed elements $x_1, \ldots, x_n$ of a commutative ring R, we can form an ideal

$$I = R \cdot x_1 + \ldots + R \cdot x_n$$

[3.0.11] **Example:** To construct new, larger ideals from old, smaller ideals proceed as follows. Let I be an ideal in a commutative ring R. Let x be an element of R. Then let

$$J = R \cdot x + I = \{rx + i : r \in R, \ \ i \in I\}$$

[15] If we do not assume that the ring is a domain, then we certainly may form the notion of *principal ideal ring*. However, the presence of zero divisors is a distraction.

[16] This is a corollary of the Euclidean-ness of $\mathbb{Z}$.

[17] This is a corollary of the Euclidean-ness of $\mathbb{Z}$.

Let's check that J is an ideal. First

$$0 = 0 \cdot x + 0$$

so 0 lies in J. Second,

$$-(rx + i) = (-r)x + (-i)$$

so J is closed under inverses. Third, for two elements $rx + i$ and $r'x + i'$ in J (with $r, r' \in R$ and $i, i' \in I$) we have

$$(rx + i) + (r'x + i') = (r + r')x + (i + i')$$

so J is closed under addition. Finally, for $rx + i \in J$ with $r \in R$, $i \in I$, and for $r' \in R$,

$$r' \cdot (rx + i) = (r'r)x + (r'i)$$

so $R \cdot J \subset J$ as required. Thus, this type of set J is indeed an ideal.

[3.0.12] **Remark:** In the case of rings such as $\mathbb{Z}$, where we know that every ideal is principal, the previous construction does not yield any more general type of ideal.

[3.0.13] **Example:** In some rings R, *not* every ideal is principal. We return to an example used earlier to illustrate a failure of unique factorization. Let

$$R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

Let

$$I = \{x \cdot 2 + y \cdot (1 + \sqrt{-5}) : x, y \in R\}$$

These phenomena are not of immediate relevance, but did provide considerable motivation in the historical development of algebraic number theory.

---

4. *Ideals and quotient rings*

Here is a construction of new rings from old in a manner that includes as a special case the construction of $\mathbb{Z}/n$ from $\mathbb{Z}$.

Let R be a commutative ring with unit 1. Let I be an ideal in R. The **quotient ring** R/I is the set of cosets

$$r + I = \{r + i : i \in I\}$$

with operations of addition and multiplication on R/I by

$$(r + I) + (s + I) = (r + s) + I$$

$$(r + I) \cdot (s + I) = (r \cdot s) + I$$

The zero in the quotient is $0_{R/I} = 0 + I$, and the unit is $1_{R/I} = 1 + I$.

[4.0.1] **Example:** The basic example is that $\mathbb{Z}/n$ is the quotient ring $\mathbb{Z}/I$ where $I = n \cdot \mathbb{Z}$.

[4.0.2] **Remark:** It's tedious, but someone should check that the operations of addition and multiplication in $\mathbb{Z}/n$ are *well-defined*: we want the alleged addition and multiplication operations not to depend on the way the coset is *named*, but only on *what it is*. So suppose $r + I = r' + I$ and $s + I = s' + I$. We need to check that

$$(r + s) + I = (r' + s') + I$$

and to prove well-definedness of multiplication check that

$$(r \cdot s) + I = (r' \cdot s') + I$$

Since $r' + I = r + I$, in particular $r' = r' + 0 \in r + I$, so r' can be written as $r' = r + i$ for some $i \in I$. Likewise, $s' = s + j$ for some $j \in I$. Then

$$(r' + s') + I = (r + i + s + j) + I = (r + s) + (i + j + I)$$

The sum $k = i + j$ is an element of I. We claim that for any $k \in I$ we have $k + I = I$. Certainly since I is closed under addition, $k + I \subset I$. On the other hand, for any $x \in I$ we can write

$$x = k + (x - k)$$

with $x - k \in I$, so also $k + I \supset I$. Thus, indeed, $k + I = I$. Thus,

$$(r' + s') + I = (r + s) + I$$

which proves the well-definedness of addition in the quotient ring. Likewise, looking at multiplication:

$$(r' \cdot s') + I = (r + i) \cdot (s + j) + I = (r \cdot s) + (rj + si + I)$$

Since I is an ideal, rj and si are again in I, and then $rj + si \in I$. Therefore, as just observed in the discussion of addition, $rj + si + I = I$. Thus,

$$(r' \cdot s') + I = (r \cdot s) + I$$

and multiplication is well-defined. The proofs that $0 + I$ is the zero and $1 + I$ is the unit are similar.

The **quotient homomorphism**

$$q : R \longrightarrow R/I$$

is the natural map

$$q(r) = r + I$$

The definition and discussion above proves

[4.0.3] **Proposition:** For a commutative ring R and ideal I, the quotient map $R \longrightarrow R/I$ is a (surjective) ring homomorphism. ///

---

5. *Maximal ideals and fields*

Now we see how to make fields by taking quotients of commutative rings by *maximal ideals* (defined just below). This is a fundamental construction.

Let R be a commutative ring with unit 1. [18] An ideal M in R is **maximal** if $M \neq R$ and if for any other ideal I with $I \supset M$ it must be that $I = R$. That is, M is a maximal ideal if there is no ideal strictly larger than M (containing M) except R itself.

[5.0.1] **Proposition:** For a commutative ring R with unit, and for an ideal I, the quotient ring R/I is a *field* if and only if I is a *maximal* ideal.

[18] The commutativity allows us to avoid several technical worries which are not the current point, and the presence of 1 likewise skirts some less-than-primary problems. The applications we have in mind of the results of this section do not demand that we worry about those possibilities.

Proof: Let $x + I$ be a non-zero element of R/I. Then $x + I \neq I$, so $x \notin I$. Note that the ideal $Rx + I$ is therefore strictly larger than I. Since I was already maximal, it must be that $Rx + I = R$. Therefore, there are $r \in R$ and $i \in I$ so that $rx + i = 1$. Looking at this last equation modulo I, we have $rx \equiv 1 \bmod I$. That is, $r + I$ is the multiplicative inverse to $x + I$. Thus, R/I is a field.

On the other hand, suppose that R/I is a field. Let $x \in R$ but $x \notin I$. Then $x + I \neq 0 + I$ in R/I. Therefore, $x + I$ has a multiplicative inverse $r + I$ in R/I. That is,

$$(r + I) \cdot (x + I) = 1 + I$$

From the definition of the multiplication in the quotient, this is $rx + I = 1 + I$, or $1 \in rx + I$, which implies that the ideal $Rx + I$ is R. But $Rx + I$ is the smallest ideal containing I and x. Thus, there cannot be any proper ideal strictly larger than I, so I is maximal. ///

6. *Prime ideals and integral domains*

Let R be a commutative ring with unit 1. An ideal P in R is **prime** if $ab \in P$ implies either $a \in P$ or $b \in P$. [19]

[6.0.1] **Proposition:** For a commutative ring R with unit, and for an ideal I, the quotient ring R/I is an *integral domain* [20] if and only if I is a *prime* ideal.

Proof: Let I be prime. Suppose that

$$(x + I) \cdot (y + I) = 0 + I$$

Recall that the product in the quotient is not defined exactly as the set of products of elements from the factors, but, rather, in effect,

$$(x + I) \cdot (y + I) = xy + I$$

Then $(x + I)(y + I) = 0 + I$ implies that $xy \in I$. By the prime-ness of I, either x or y is in I, so either $x + I = 0 + I$ or $y + I = 0 + I$.

On the other hand, suppose that R/I is an integral domain. Suppose that $xy \in I$. The definition $(x + I)(y + I) = xy + I$ then says that $(x + I)(y + I) = 0 + I$. Since R/I is an integral domain, either $x + I = I$ or $y + I = I$. That is, either $x \in I$ or $y \in I$, and I is prime. ///

[6.0.2] **Corollary:** Maximal ideals are prime. [21]

Proof: If I is a maximal ideal in a ring R, then R/I is a field, from above. Fields are certainly integral domains, so I is prime, from above. ///

[6.0.3] **Remark:** Not all prime ideals are maximal.

[6.0.4] **Example:** Let $R = \mathbb{Z}[x]$ be the polynomial ring in one variable with integer coefficients. Consider the ideal $I = \mathbb{Z}[x] \cdot x$ generated by x. We claim that this ideal is prime, but *not* maximal. Indeed,

$$R/I = \mathbb{Z}[x]/x\mathbb{Z}[x] \approx \mathbb{Z}$$

via the homomorphism

$$P(x) + I \longrightarrow P(0)$$

(One might verify that this map is indeed well-defined, and is a homomorphism.) [22] Since $\mathbb{Z} \approx \mathbb{Z}[x]/I$ is an integral domain, I is prime, but since $\mathbb{Z}$ is not a field, I is not maximal.

[6.0.5] **Example:** Let $R = \mathbb{Z}[x]$ again and let $I = \mathbb{Z}[x] \cdot p$ be the ideal generated by a prime number p. Then

$$R/I = \mathbb{Z}[x]/p\mathbb{Z}[x] \approx (\mathbb{Z}/p)[x]$$

[19] Yes, by this point the property *proven* for prime numbers is taken to be the *definition*.

[20] Again, an integral domain has no zero divisors.

[21] ... in commutative rings with identity, at least.

[22] This can be verified in different styles. One style is the following. The universality of the polynomial ring assures us that there is a unique $\mathbb{Z}$-algebra homomorphism $e : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ which sends $x \longrightarrow 0$. Implicit in the $\mathbb{Z}$-algebra homomorphism property is that $n \longrightarrow n$ for $n \in \mathbb{Z}$, so no non-zero integers lie in the kernel of this *evaluation homomorphism* e. Thus, this homomorphism is a surjection to $\mathbb{Z}$.

via the map

$$P(x) \longrightarrow (P \text{ with coefficients reduced mod } p)(x)$$

The ring $(\mathbb{Z}/p)[x]$ is an integral domain [23] but not a field, so the ideal is prime but not maximal.

[6.0.6] **Example:** [24] Let k be a field, and consider the polynomial ring $R = k[x, y]$ in two variables. Let $I = k[x, y] \cdot x$ be the ideal generated by x. We claim that this ideal I is prime but not maximal. Indeed, the quotient R/I is [25] (naturally isomorphic to) $k[y]$ under the evaluation map

$$P(x, y) \longrightarrow P(0, y)$$

Since $k[xy]$ is an integral domain but not a field, we reach the conclusion, in light of the results just above.

---

7. Fermat-Euler on sums of two squares

[7.0.1] **Theorem:** [26] A prime integer p is expressible as

$$p = a^2 + b^2$$

if and only if $p = 1 \bmod 4$ (or $p = 2$).

Proof: Parts of this are very easy. Certainly $2 = 1^2 + 1^2$. Also, if an odd [27] prime is expressible as $p = a^2 + b^2$, then, since the squares modulo 4 are just 0 and 1, it must be that one of a, b is odd and one is even, and the sum of the squares is 1 modulo 4.

On the other hand, suppose that $p = 1 \bmod 4$. If p were expressible as $p = a^2 + b^2$ then

$$p = (a + bi)(a - bi)$$

where $i = \sqrt{-1}$ in $\mathbb{C}$. That is, p is expressible as a sum of two squares, if and only if p factors in a particular manner in $\mathbb{Z}[i]$. One might have at some point already observed that the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$, so if neither of a, b is 0, then neither of $a \pm bi$ is a unit. We need to analyze the possible factorization of p in $\mathbb{Z}[i]$ a little more closely to understand the close connection to the present issue.

---

[23] Since p is prime, $\mathbb{Z}/p$ is a field, so this is a polynomial ring in one variable over a field, which we know is an integral domain.

[24] While the conclusion of this example is correct, the most natural full proof that such things are what they seem requires results we do not yet have in hand, such as Gauss' Lemma.

[25] Certainly if we have a polynomial of the form $xf(x, y)$, replacing x by 0 gives the 0 polynomial in y. On the other hand, it is less clear that $f(0, y) = 0$ implies that f is of the form $f(x, y) = xg(x, y)$ for some polynomial g. The conceptual proof of results of this sort would use the unique factorization property of $k[x, y]$, which follows from the one-variable case via Gauss' lemma. For the present case, with the special factor x (rather than a more general polynomial), a direct approach is still easy. Let $f(x, y) = xg(x, y) + h(x)$ where $h(y)$ is the collection of all monomials in $f(x, y)$ in which x does not appear. Then $f(0, y) = h(y)$. If this is the 0 polynomial in y, then $f(x, y) = xg(x, y)$.

[26] Fermat stated in correspondence that he knew this, roughly around 1650, but there was no recorded argument. About 100 years later Euler reconsidered this and many other unsupported statements of Fermat's, and gave a proof that was publicly available. In this and other cases, it is not clear that Fermat was sufficiently aware of all the things that might go wrong to enable us to be sure that he had a complete proof. It is plausible, but not clear.

[27] The phrase *odd prime* is a standard if slightly peculiar way to refer to prime integers other than 2. Sometimes the import of this is that the prime is *larger* than 2, and sometimes it really is that the prime is *odd*.

Let $N(a+bi) = a^2+b^2$ be the usual (square-of) norm. One can check that the only elements of $\mathbb{Z}[i]$ with norm 1 are the 4 units, and norm 0 occurs only for 0. If $p = \alpha \cdot \beta$ is a proper factorization, then by the multiplicative property of N

$$p^2 = N(p) = N(\alpha) \cdot N(\beta)$$

Thus, since neither α nor β is a unit, it must be that

$$N(\alpha) = p = N(\beta)$$

Similarly, α and β must both be irreducibles in $\mathbb{Z}[i]$, since applying N to any proper factorization would give a contradiction. Also, since p is its own complex conjugate,

$$p = \alpha \cdot \beta$$

implies

$$p = \overline{p} = \overline{\alpha} \cdot \overline{\beta}$$

Since we know that the Gaussian integers $\mathbb{Z}[i]$ are Euclidean and, hence, have unique factorization, it must be that these two prime factors are the same *up to units*. [28]

Thus, either $\alpha = \pm\overline{\alpha}$ and $\beta = \pm\overline{\beta}$ (with matching signs), or $\alpha = \pm i\overline{\alpha}$ and $\beta = \mp i\overline{\beta}$, or $\alpha = u\overline{\beta}$ with u among $\pm 1, \pm i$. If $\alpha = \pm\overline{\alpha}$, then α is either purely imaginary or is real, and in either case its norm is a square, but no square divides p. If $\alpha = \pm i\overline{\alpha}$, then α is of the form $t \pm it$ for $t \in \mathbb{Z}$, and then $N(\alpha) \in 2\mathbb{Z}$, which is impossible.

Thus, $\alpha = u\overline{\beta}$ for some unit u, and $p = uN(\beta)$. Since $p > 0$, it must be that $u = 1$. Letting $\alpha = a + bi$, we have recovered an expression as (proper) sum of two squares

$$p = a^2 + b^2$$

Thus, a prime integer p is a (proper) sum of two squares if and only if it is *not prime* in $\mathbb{Z}[i]$. From above, this is equivalent to

$$\mathbb{Z}[i]/p\mathbb{Z}[x] \text{ is not an integral domain}$$

We grant that for $p = 1 \bmod 4$ there is an integer α such that $\alpha^2 = -1 \bmod p$. [29] That is, (the image of) the polynomial x^2+1 factors in $\mathbb{Z}/p[x]$.

Note that we can rewrite $\mathbb{Z}[i]$ as

$$\mathbb{Z}[x]/(x^2+1)\mathbb{Z}[x]$$

We'll come back to this at the end of this discussion. Then [30]

$$\mathbb{Z}[i]/\langle p\rangle \approx \left(\mathbb{Z}[x]/\langle x^2+1\rangle\right)/\langle p\rangle$$

[28] This *up to units* issue is nearly trivial in $\mathbb{Z}$, since positivity and negativity give us a convenient handle. But in $\mathbb{Z}[i]$ and other rings with more units, greater alertness is required.

[29] If we grant that there are primitive roots modulo primes, that is, that $(\mathbb{Z}/p)^\times$ is cyclic, then this assertion follows from basic and general properties of cyclic groups. Even without knowledge of primitive roots, we can still give a special argument in this limited case, as follows. Let $G = (\mathbb{Z}/p)^\times$. This group is abelian, and has order divisible by at least 2^2. Thus, for example by Sylow theorems, there is a 2-power-order subgroup A of order at least 4. By unique factorization in polynomial rings, the equation $x^2 - 1 = 0$ has only the solutions ± 1. Thus, there is only a *single* element in A of order 2, and the identity 1 of order 1. Other elements in A must have order a larger power of 2, and then one can arrange elements of order 4. Such things would be 4^{th} roots of 1.

[30] A scrupulous reader should verify that the change in order of quotient-taking is legitimate. It is certainly a good trick, assuming that it works properly.

$$\approx (\mathbb{Z}[x]/\langle p\rangle)\,/\langle x^2+1\rangle \approx (\mathbb{Z}/p)[x]/\langle x^2+1\rangle$$

and the latter is *not* an integral domain, since

$$x^2+1 = (x-\alpha)(x+\alpha)$$

is not irreducible in $(\mathbb{Z}/p)[x]$. That is, $\mathbb{Z}[i]/\langle p\rangle$ is not an integral domain when p is a prime with $p = 1 \bmod 4$. That is, p is not irreducible in $\mathbb{Z}[i]$, so factors properly in $\mathbb{Z}[i]$, thus, as observed above, p is a sum of two squares. ///

[7.0.2] **Remark:** Let's follow up on the isomorphism

$$\mathbb{Z}[x]/\langle x^2+1\rangle \approx \mathbb{Z}[i]$$

Since $\mathbb{Z}[x]$ is the free $\mathbb{Z}$-algebra on the generator x, there is a unique $\mathbb{Z}$-algebra homomorphism $\mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$ taking x to i. We claim that the kernel is identifiable as the principal ideal generated by x^2+1, after which the obvious isomorphism theorem for rings would yield the desired isomorphism.

That is, we claim that if a polynomial $P(x)$ in $\mathbb{Z}[x]$ has the property that $P(i) = 0$, then P is a multiple (in $\mathbb{Z}[x]$) of x^2+1. This is less trivial than in the case of polynomials in one variable over a *field*, but the fact that x^2+1 is *monic* saves us. That is, we can claim that for a *monic* poly $M(x)$, given any other polynomial $P(x) \in \mathbb{Z}[x]$, there are $Q(x)$ and $R(x)$ in $\mathbb{Z}[x]$ with $\deg R < \deg M$, such that

$$P = Q \cdot M + R$$

Indeed, suppose not. Let

$$P(x) = a_n x^n + \ldots + a_0$$

be the polynomial of least degree n which we cannot divide by M and obtain a smaller remainder. Let $m = \deg M$. Necessarily $n \geq m$ or P is itself already of lower degree than M. And, for $n \geq m$,

$$P - a_n \cdot x^{n-m} \cdot M$$

is of strictly lower degree than P, so is expressible as $QM + R$. Then

$$P = (Q + a_n x^{n-m}) \cdot M + R$$

Since the degree of R was of degree at most $n-1$, which is strictly less than n, this contradicts the supposition that P had no such expression.

---

8. *Worked examples*

[4.1] Let $R = \mathbb{Z}/13$ and $S = \mathbb{Z}/221$. Show that the map

$$f : R \longrightarrow S$$

defined by $f(n) = 170 \cdot n$ is *well-defined* and is a ring homomorphism. (Observe that it does not map $1 \in R$ to $1 \in S$.)

The point is that $170 = 1 \bmod 13$ and $170 = 17 \cdot 10 = 0 \bmod 17$, and $221 = 13 \cdot 17$. Thus, for $n' = n + 13\ell$,

$$170 \cdot n' = 17 \cdot 10 \cdot n + 10 \cdot 17 \cdot 13 = 17 \cdot 10 \cdot n \bmod 13 \cdot 17$$

so the map is well-defined. Certainly the map respects addition, since

$$170(n+n') = 170n + 170n'$$

That it respects multiplication is slightly subtler, but we verify this separately modulo 13 and modulo 17, using unique factorization to know that if $13|N$ and $17|N$ then $(13 \cdot 17)|N$. Thus, since $170 = 1 \bmod 13$,

$$170(nn') = 1 \cdot (nn') = nn' = (170n) \cdot (170n') \bmod 13$$

And, since $17 = 0 \bmod 17$,

$$170(nn') = 0 \cdot (nn') = 0 = (170n) \cdot (170n') \bmod 17$$

Putting these together gives the multiplicativity.

[4.2] Let p and q be distinct prime numbers. Show directly that there is no field with pq elements.

There are several possible approaches. One is to suppose there exists such a field k, and first invoke Sylow (or even more elementary results) to know that there exist (non-zero!) elements x, y in k with (additive) orders p, q, respectively. That is, $p \cdot x = 0$ (where left multiplication by an ordinary integer means repeated addition). Then claim that $xy = 0$, contradicting the fact that a field (or even integral domain) has no proper zero divisors. Indeed, since p and q are distinct primes, $\gcd(p, q) = 1$, so there are integers r, s such that $rp + sq = 1$. Then

$$xy = 1 \cdot xy = (rp + sq) \cdot xy = ry \cdot px + sx \cdot qy = ry \cdot 0 + sx \cdot 0 = 0$$

[4.3] Find all the idempotent elements in $\mathbb{Z}/n$.

The idempotent condition $r^2 = r$ becomes $r(r-1) = 0$. For each prime p dividing n, let p^e be the exact power of p dividing n. For the image in $\mathbb{Z}/n$ of an ordinary integer b to be idempotent, it is necessary and sufficient that $p^e|b(b-1)$ for each prime p. Note that p cannot divide both b and $b-1$, since $b-(b-1) = 1$. Thus, the condition is $p^e|b$ *or* $p^e|b-1$, for each prime p dividing n. Sun-Ze's theorem assures that we can choose either of these two conditions for each p as p various over primes dividing n, and be able to find a simultaneous solution for the resulting family of congruences. That is, let $p_1, \ldots, p_t$ be the distinct primes dividing n, and let $p_i^{e_i}$ be the exact power of p_i dividing n. For each p_i choose $\varepsilon_i \in \{0, 1\}$. Given a sequence $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_t)$ of 0s and 1s, consider the collection of congruences $p_i^{e_i}|(b - \varepsilon_i)$, for $i = 1, \ldots, t$. Sun-Ze guarantees that there is a solution, and that it is unique mod n. Thus, each of the 2^t choices of sequences of 0s and 1s gives an idempotent.

[4.4] Find all the nilpotent elements in $\mathbb{Z}/n$.

For each prime p dividing n, let p^e be the exact power of p dividing n. For the image in $\mathbb{Z}/n$ of an ordinary integer b to be nilpotent, it is necessary and sufficient that for some n sufficiently large $p^e|b^n$ for each prime p. Then surely $p|b^n$, and since p is prime $p|b$. And, indeed, if every prime dividing n divides b, then a sufficiently large power of b will be 0 modulo p^e, hence (by unique factorization, etc.) modulo n. That is, for b to be nilpotent it is necessary and sufficient that every prime dividing n divides b.

[4.5] Let $R = \mathbb{Q}[x]/(x^2 - 1)$. Find e and f in R, neither one 0, such that

$$e^2 = e \quad f^2 = f \quad ef = 0 \quad e + f = 1$$

(Such e and f are **orthogonal** idempotents.) Show that the maps $p_e(r) = re$ and $p_f(r) = rf$ are ring homomorphisms of R to itself.

Let ξ be the image of x in the quotient. Then $(\xi - 1)(\xi + 1) = 0$. Also note that

$$(\xi - 1)^2 = \xi^2 - 2\xi + 1 = (\xi^2 - 1) - 2\xi + 2 = -2\xi + 2$$

so

$$\left(\frac{\xi-1}{2}\right)^2 = \frac{\xi^2-2\xi+1}{4} = \frac{(\xi^2-1)-2\xi+2}{4} = \frac{-\xi+1}{2}$$

Similarly,

$$\left(\frac{\xi+1}{2}\right)^2 = \frac{\xi^2+2\xi+1}{4} = \frac{(\xi^2-1)+2\xi+2}{4} = \frac{\xi+1}{2}$$

Thus, $e = (-\xi+1)/2$ and $f = (\xi+1)/2$ are the desired orthogonal idempotents.

[4.6] Prove that in $(\mathbb{Z}/p)[x]$ we have the factorization

$$x^p - x = \prod_{a\in\mathbb{Z}/p} (x-a)$$

By Fermat's Little Theorem, the left-hand side is 0 when x is replaced by any of $0, 1, 2, \ldots, p-1$. Thus, by unique factorization in $k[x]$ for k a field (which applies to $\mathbb{Z}/p$ since p is prime), all the factors $x-0$, $x-1$, $x-2$, ..., $x-(p-1)$ divide the left-hand side, and (because these are mutually relatively prime) so does their product. Their product is the right-hand side, which thus at least *divides* the left-hand side. Since degrees add in products, we see that the right-hand side and left-hand side could differ at most by a unit (a polynomial of degree 0), but both are *monic*, so they are identical, as claimed.

[4.7] Let $\omega = (-1+\sqrt{-3})/2$. Prove that

$$\mathbb{Z}[\omega]/p\mathbb{Z}[\omega] \approx (\mathbb{Z}/p)[x]/(x^2+x+1)(\mathbb{Z}/p)[x]$$

and, as a consequence, that a prime p in $\mathbb{Z}$ is expressible as x^2+xy+y^2 with integers x, y if and only if $p = 1 \bmod 3$ (apart from the single anomalous case $p = 3$).

If a prime is expressible as $p = a^2+ab+b^2$, then, modulo 3, the possibilities for p modulo 3 can be enumerated by considering $a = 0, \pm 1$ and $b = 0, \pm 1 \bmod 3$. Noting the symmetry that $(a, b) \longrightarrow (-a, -b)$ does not change the output (nor does $(a, b) \longrightarrow (b, a)$) we reduce from $3 \cdot 3 = 9$ cases to a smaller number:

$$p = a^2+ab+b^2 = \begin{cases} 0^2+0\cdot 0+0^2 & = & 1 & \bmod 3 \\ 1^2+1\cdot 1+1^2 & = & 0 & \bmod 3 \\ 1^2+1\cdot(-1)+(-1)^2 & = & 1 & \bmod 3 \end{cases}$$

Thus, any prime p expressible as $p = a^2+ab+b^2$ is either 3 or is 1 mod 3.

On the other hand, suppose that $p = 1 \bmod 3$. If p were expressible as $p = a^2+ab+b^2$ then

$$p = (a+b\omega)(a+b\overline{\omega})$$

where $\omega = (-1+\sqrt{-3})/2$. That is, p is expressible as a^2+ab+b^2 if and only if p factors in a particular manner in $\mathbb{Z}[\omega]$.

Let $N(a+b\omega) = a^2+ab+b^2$ be the usual (square-of) norm. To determine the units in $\mathbb{Z}[\omega]$, note that $\alpha\cdot\beta = 1$ implies that

$$1 = N(\alpha)\cdot N(\beta)$$

and these norms from $\mathbb{Z}[\omega]$ are integers, so units have norm 1. By looking at the equation $a^2+ab+b^2 = 1$ with integers a, b, a little fooling around shows that the only units in $\mathbb{Z}[\omega]$ are ± 1, $\pm\omega$ and $\pm\omega^2$. And norm 0 occurs only for 0.

If $p = \alpha\cdot\beta$ is a proper factorization, then by the multiplicative property of N

$$p^2 = N(p) = N(\alpha)\cdot N(\beta)$$

Thus, since neither α nor β is a unit, it must be that

$$N(\alpha) = p = N(\beta)$$

Similarly, α and β must both be irreducibles in $\mathbb{Z}[\omega]$, since applying N to any proper factorization would give a contradiction. Also, since p is its own complex conjugate,

$$p = \alpha \cdot \beta$$

implies

$$p = \overline{p} = \overline{\alpha} \cdot \overline{\beta}$$

Since we know that the (Eisenstein) integers $\mathbb{Z}[\omega]$ are Euclidean and, hence, have unique factorization, it must be that these two prime factors are the same *up to units*.

Thus, either $\alpha = \pm\overline{\alpha}$ and $\beta = \pm\overline{\beta}$ (with matching signs), or $\alpha = \pm\omega\overline{\alpha}$ and $\beta = \pm\omega^2\overline{\beta}$, or $\alpha = \pm\omega^2\overline{\alpha}$ and $\beta = \pm\omega\overline{\beta}$, or $\alpha = u\overline{\beta}$ with u among $\pm 1, \pm\omega, \pm\omega^2$. If $\alpha = \pm\overline{\alpha}$, then α is either in $\mathbb{Z}$ or of the form $t \cdot \sqrt{-3}$ with $t \in \mathbb{Z}$. In the former case its norm is a square, and in the latter its norm is divisible by 3, neither of which can occur. If $\overline{\alpha} = \omega\alpha$, then $\alpha = t \cdot \omega$ for some $t \in \mathbb{Z}$, and its norm is a square, contradiction. Similarly for $\alpha = \pm\omega^2\overline{\alpha}$.

Thus, $\alpha = u\overline{\beta}$ for some unit u, and $p = uN(\beta)$. Since $p > 0$, it must be that $u = 1$. Letting $\alpha = a + b\omega$, we have recovered an expression

$$p = a^2 + ab + b^2$$

with neither a nor b zero.

Thus, a prime integer $p > 3$ is expressible (properly) as $a^2 + ab + b^2$ of two squares if and only if it is *not prime* in $\mathbb{Z}[\omega]$. From above, this is equivalent to

$$\mathbb{Z}[\omega]/\langle p\rangle \text{ is not an integral domain}$$

We grant that for $p = 1 \bmod 3$ there is an integer α such that $\alpha^2 + alf + 1 = 0 \bmod p$. [31] That is, (the image of) the polynomial $x^2 + x + 1$ factors in $(\mathbb{Z}/p)[x]$.

Note that we can rewrite $\mathbb{Z}[\omega]$ as

$$\mathbb{Z}[x]/\langle x^2 + x + 1\rangle$$

Then

$$\mathbb{Z}[\omega]/\langle p\rangle \approx \left(\mathbb{Z}[x]/\langle x^2+1\rangle\right)/\langle p\rangle \approx \left(\mathbb{Z}[x]/\langle p\rangle\right)/\langle x^2+1\rangle \approx (\mathbb{Z}/p)[x]/\langle x^2+1\rangle$$

and the latter is *not* an integral domain, since

$$x^2 + x + 1 = (x - \alpha)(x - \alpha^2)$$

is not irreducible in $(\mathbb{Z}/p)[x]$. That is, $\mathbb{Z}[\omega]/\langle p\rangle$ is not an integral domain when p is a prime with $p = 1 \bmod 3$. That is, p is not irreducible in $\mathbb{Z}[\omega]$, so factors properly in $\mathbb{Z}[\omega]$, thus, as observed above, p is expressible as $a^2 + ab + b^2$. ///

[31] If we grant that there are primitive roots modulo primes, that is, that $(\mathbb{Z}/p)^\times$ is cyclic, then this assertion follows from basic and general properties of cyclic groups. Even without knowledge of primitive roots, we can still give a special argument in this limited case, as follows. Let $G = (\mathbb{Z}/p)^\times$. This group is abelian, and has order divisible by 3. Thus, for example by Sylow theorems, there is a 3-power-order subgroup A, and, thus, at least one element of order exactly 3.

Exercises

4.[8.0.1] Show that in a commutative ring the set of nilpotent elements is an ideal (the **nilradical** of R). Give an example to show that the set of nilpotent elements may fail to be an ideal in a non-commutative ring.

4.[8.0.2] Let R be a commutative ring with unit, such that for every $r \in R$ there is an integer $n > 1$ (possibly depending upon r) such that $r^n = r$. Show that every prime ideal in R is maximal.

4.[8.0.3] Let k be a field. Let P, Q be two polynomials in $k[x]$. Let K be an extension field of k. Show that, if P divides Q in $K[x]$, then P divides Q in $k[x]$.

4.[8.0.4] Let R be a commutative ring with unit. Show that the set of prime ideals in R has minimal elements under the ordering by inclusion. (*Hint:* You may want to use Zorn's lemma or some other equivalent of the Axiom of Choice.)

4.[8.0.5] The **radical** of an ideal I in a commutative ring R with unit is

$$\operatorname{rad} I = \{r \in R : r^n \in I \text{ for some } n\}$$

Show that a proper ideal I of a ring is equal to its own radical if and only if it is an intersection of prime ideals.

4.[8.0.6] Let R be a commutative ring with unit. Check that the **nilradical** N of R, defined to be the set of all nilpotent elements, is

$$\operatorname{nilrad} R = \operatorname{rad} \{0\}$$

Show that R has a *unique* prime ideal if and only if every element of R is either nilpotent or a unit, if and only if R/N is a field.

4.[8.0.7] Show that a prime p in $\mathbb{Z}$ is expressible as $p = m^2 + 2n^2$ with integers m, n if and only if -2 is a square mod p.

4.[8.0.8] Let R be a commutative ring with unit. Suppose R contains an *idempotent* element r other than 0 or 1. (That is, $r^2 = r$.) Show that every prime ideal in R contains an idempotent other than 0 or 1.