1 MATH 340 Notes and Exercises for Ideals

Michael Monagan, November 2017
If you find any errors please let me know: `mmonagan@cecm.sfu.ca`

1.1 Definition and Examples

We begin with the definition of an ideal in a commutative ring. Ideals in non-commutative rings can be defined but we will not study them here.

Definition 1.1.1. *Let R be a commutative ring. A subset of I of R is an* ideal *of R if*

(i) $0_R \in I$,

(ii) if $a, b \in I$ *then* $a - b \in I$, *and*

(iii) if $a \in I$ *and* $r \in R$ *then* $ar = ra \in I$.

Observe that the set $I = \{0_R\}$ is an ideal of R. Also, the entire ring R is an ideal of R. These two ideals are called the trivial ideals. An example of non-trivial ideal is the set of even integers.

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

This is an ideal in $\mathbb{Z}$ because if a, b are even integers, and r is any integer, we have $a - b$ is even and ar is even. Now the even integers are also a subring of $\mathbb{Z}$. There is a relation between ideals and subrings, namely, all ideals are subrings but not all subrings are ideals. We recall the test for a subring of a ring. See Lemma 2.2.4.

Subring Test Let R be a ring. A subset of S of R is a subring of R if

(1) S is not empty,

(2) if $a, b \in S$ then $-a \in S$ and $a + b \in S$, and

(3) if $a, b \in S$ then $ab \in S$.

Some texts will have $0_R \in S$ instead of S is not empty for condition (1). The two conditions are in fact equivalent. Furthermore condition (2) in the test for a subring and condition (ii) in the definition for an ideal are also equivalent conditions. Let us state and prove this formally.

Lemma 1.1.2. *Let S and I be as above. Then (i) S is closed under subtraction and (ii) I is closed under addition and negation.*

Proof. (i) Let $a, b \in S$. Then $a - b = a + (-b)$. Since $-b \in S$ and S is closed under addition thus $a - b \in S$. (ii) Let $a, b \in I$. Then $0_R - a \in I$. But $0_R - a = -a \in I$ thus I is closed under negation. Also $a + b = a - (-b) = a - (0_R - b) \in I$. Thus I is closed under addition. □

Property (iii) in the definition for ideals means I is closed under multiplication hence every ideal in R is a subring. However, it is not the case that every subring is an ideal. The following Lemma leads to such examples.

Lemma 1.1.3. *Let R be a commutative ring with identity and let I be an ideal in R. If a unit $u \in I$ then $I = R$.*

Proof. Let y be the inverse of u. Then $yu \in I$ by (iii) and $yu = 1$. But $1 \in I$ implies all elements are of R are in I by (iii). That is, $R \subset I$ and hence $I = R$. □

It follows that if R is a field then the only ideals in R are the trivial ideals $\{0_R\}$ and R. We have seen examples where a field F can have a proper subfields. For example, GF(16) has a subfields GF(2) and GF(4). Also $\mathbb{Z}$ is the constant subring of $\mathbb{Z}[x]$ but $\mathbb{Z}$ is not an ideal in $\mathbb{Z}[x]$.

We now consider how to construct ideals from elements in R.

Definition 1.1.4. *Let R be a commutative ring. For $a \in R$ let us define*

$$\langle a \rangle = \{ab : b \in R\}$$

which is all multiplies of a by R. More generally, for $a_1, \ldots, a_n \in R$ let us define

$$\langle a_1, \ldots, a_n \rangle = \{\textstyle\sum_{i=1}^n a_i b_i \ : \ b_i \in R\}.$$

Lemma 1.1.5 below proves that these sets are ideals in R. The set $\langle a_1, \ldots, a_n \rangle$ is called the ideal generated by $\{a_1, ..., a_n\}$ and the elements $\{a_1, ..., a_n\}$ are called generators. An ideal $\langle a \rangle$ generated by a single element a is called a principle ideal. It turns out that all ideals in $\mathbb{Z}$ and $F[x]$ where F is a field are principle ideals.

Lemma 1.1.5. *Let R be a commutative ring. The set $I = \langle a_1, \ldots, a_n \rangle$ is an ideal of R.*

Proof. We must prove properties (i), (ii) and (iii) for an ideal.

(i) Take $b_i = 0_R$. Then $\sum_{i=1}^n a_i b_i = \sum_{i=1}^n a_i 0_R = 0_R$. Since the sum is in I by definition of $\langle\ \rangle$ we have $0_R \in I$.

(ii) Let f and g be in I. Then $f = \sum_{i=1}^n a_i f_i$ for some $f_i \in R$ and $g = \sum_{i=1}^n a_i g_i$ for some $g_i \in R$. Now $f - g = \sum_{i=1}^n a_i f_i - \sum_{i=1}^n a_i g_i = \sum_{i=1}^n a_i (f_i - g_i) \in I$ since $f_i - g_i \in R$.

(iii) Let f be in I and $h \in R$. Then $f = \sum_{i=1}^n a_i f_i$ for some $f_i \in R$. Now $hf = fh = \sum_{i=1}^n (a_i f_i) h = \sum_{i=1}^n a_i (f_i h) \in I$ since $f_i h \in R$.

□

In $\mathbb{Z}$ the ideal $\langle 6\rangle = \{6b : b \in \mathbb{Z}\}$ is all multiples of 6. In $\mathbb{Q}[x]$ the ideal $\langle x\rangle = \{fx : f \in \mathbb{Q}[x]\}$ is all polynomials in $\mathbb{Q}[x]$ divisible by x.

Example 1.1.6. *Find all ideals in $\mathbb{Z}_6$. One way to do this is to start with $\{0\}$ and consider including each non-zero element of $\mathbb{Z}_6$ and adding elements until the set is closed under $+$ and see if we have an ideal. We get the following ideals*

$$\begin{array}{c|l} 0 & \{0\} = \langle 0\rangle \\ 1 & \{0,1,1+1=2,1+2=3,1+3=4,1+4=5\} = \langle 1\rangle \\ 2 & \{0,2,2+2=4\} = \langle 2\rangle \\ 3 & \{0,3\} = \langle 3\rangle \\ 4 & \{0,4,4+4=2\} = \langle 2\rangle \\ 5 & \{0,5,5+5=4,5+4=3,5+3=2,5+2=1\} = \langle 1\rangle \end{array}$$

Thus we obtain the trivial ideals $\langle 0\rangle$, $\langle 1\rangle$ and non-trivial ideals $\langle 2\rangle$, $\langle 3\rangle$ and conclude that all ideals in $\mathbb{Z}_6$ are principle ideals. And we observe a one to one correspondence between the subrings of $\mathbb{Z}_6$ and the ideals of $\mathbb{Z}_6$.

Lemma 1.1.7. *(basic properties of generators)*
Let R be a commutative ring and let $a, b \in R$ and let u be a unit in R. Then

(i) $\langle a, ab\rangle = \langle a\rangle$.

(ii) $\langle ua\rangle = \langle a\rangle$, *in particular* $\langle -a\rangle = \langle a\rangle$.

(iii) $\langle a, b, a+b\rangle = \langle a, b\rangle$.

Proof. To prove (i) let $I = \langle a, ab\rangle$ and let $J = \langle a\rangle$. ($I \subset J$) Let $c \in I \Rightarrow c = xa + yab$ for some $x, y \in R$. Now $xa + yab = (x + yb)a \in J$. ($J \subset I$) Let $c \in J \Rightarrow c = xa$ for some $x \in R$. Now $xa = xa + 0ab \Rightarrow c \in I$. The proofs of (ii) and (iii) are left to the exercises. □

1.1.1 Ideals in $\mathbb{Z}$

Theorem 1.1.8. *Every ideal in $\mathbb{Z}$ is of the form $\langle a\rangle$ for some non-negative integer a.*

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = \{0\}$ then $I = \langle 0\rangle$ and the theorem is true. If $I \neq \{0\}$ then I has at least one non-zero element x. Since I is closed under subtraction then $0 - x \in I$ thus I must have at least one positive and one negative integer. Let b be the least positive integer in I. We claim $I = \langle b\rangle$. Let a be any other element in I. We just need to show $a \in \langle b\rangle$. Dividing a by b we obtain integers q and r satisfying

$$a = bq + r \text{ with } 0 \leq r < b.$$

We have $r = a - bq$. But $a, b \in I \Rightarrow a - bq \in I \Rightarrow r \in I$. If $0 < r < b$ then we have a smaller positive element than b in I, a contradiction. Thus $r = 0$ and $a = bq$ and thus $a \in \langle b\rangle$. □

Example 1.1.9. *According to Theorem 1.1.8 the ideal* $\langle 6,4\rangle = \langle b\rangle$ *for some positive integer* b. I *is an ideal so* $6-4=2\in I$ *since* I *is closed under subtraction. Let* $J=\langle 2\rangle$. *We claim* $I=J$. *To prove* $I\subset J$ *let* $c\in I$. *Then* $c=6x+4y$ *for some integers* x,y. *Clearly* $2|6x+4y$ *so* $c\in\langle 2\rangle$. *To prove* $J\subset I$ *let* $c\in J$ *so* $c=2z$ *for some integer* z. *Now* $2z=6z-4z=6z+4(-z)\in I$. *Observe that* $2=\gcd(6,4)$.

Theorem 1.1.10. *Let* $a,b\in\mathbb{Z}$ *be nonzero and let* $I=\langle a,b\rangle$. *Then* $I=\langle g\rangle$ *where* $g=\gcd(a,b)$.

Proof. ($I\subset\langle g\rangle$) Let f be in I. Then $f=ax+by$ for some $x,y\in\mathbb{Z}$. But $g=\gcd(a,b)\Rightarrow g|a$ and $g|b$ which implies $g|f\Rightarrow f\in\langle g\rangle$.

($\langle g\rangle\subset I$) Let h be in $\langle g\rangle$. Thus $h=gq$ for some integer q. By the extended Euclidean algorithm there exist integers s,t such that $sa+tb=g$. Thus $h=gq=(sa+tb)q=a(qs)+b(qt)\in I$. □

Theorem 1.1.10 generalizes so that $\langle 30,-20,45\rangle=\langle\gcd(30,-20,45)\rangle=\langle 5\rangle$.

Corollary 1.1.11. *Let* $a_1,a_2,\dots,a_n$ *be* $n\ge 2$ *non-zero integers.*
Then $I=\langle a_1,a_2,\dots,a_n\rangle=\langle g\rangle$ *where* $g=\gcd(a_1,a_2,\dots,a_n)$.

Proof. (by induction on n) Induction base ($n=2$): see Theorem 1.1.10.
Induction step ($n>2$): Let $h=\gcd(a_1,\dots,a_{n-1})$. Assume $\langle a_1,\dots,a_{n-1}\rangle=\langle h\rangle$. Now by definition of $\langle\ \rangle$, $I=\{\sum_{i=1}^n a_ib_i\}$ for some integers b_i. We have

$$\begin{aligned} I &= \{\textstyle\sum_{i=1}^n a_ib_i : b_i\in\mathbb{Z}\}\\ &= \left\{a_nb_n+\textstyle\sum_{i=1}^{n-1} a_ib_i : b_i\in\mathbb{Z}\right\}\\ &= \{a_nb_n+hb : b_n,b\in\mathbb{Z}\}\ \text{ by induction on } n.\\ &= \langle a_n,h\rangle\\ &= \langle\gcd(h,a_n)\rangle\ \text{ by Theorem 1.1.10.}\end{aligned}$$

Finally $\gcd(h,a_n)=\gcd(\gcd(a_1,\dots,a_{n-1}),a_n)=\gcd(a_1,a_2,\dots,a_n)=g$. □

We end with some examples of constructing new ideals from old ideals.

Lemma 1.1.12. *Let* I *and* J *be two ideals in a commutative ring* R. *Let* $I+J=\{a+b : a\in I \text{ and } b\in J\}$ *denote the sum of two ideals. Then* $I\cap J$ *and* $I+J$ *are ideals in* R.

The proof is left as an exercise. As an example consider $I=\langle 6\rangle$ and $J=\langle 4\rangle$ in $\mathbb{Z}$. Now $I=\{0,\pm6,\pm12,\pm18,\pm24,\dots\}$ and $J=\{0,\pm4,\pm8,\pm12,\pm16,\pm20,\pm24,\dots\}$. We see that $I\cap J=\{0,\pm12,\pm24,\dots\}=\langle 12\rangle=\langle\operatorname{lcm}(6,4)\rangle$. Also $I+J$ includes $6+(-4)=2$ and the elements of $I+J$ are of the form $6x+4y$ which are all even hence $I+J=\langle 2\rangle=\langle\gcd(6,4)\rangle$.

1.2 Maximal Ideals

Definition 1.2.1. *An ideal I in a commutative ring R is said to be* maximal *if there is no ideal J lying strictly between I and R, that is, $I \subset J \subset R$ with $I \neq J$ and $J \neq R$.*

We have $\langle 6 \rangle \subset \langle 3 \rangle \subset \langle 1 \rangle = \mathbb{Z}$. Is there any ideal strictly between $\langle 3 \rangle$ and $\mathbb{Z}$? The next Lemma says $\langle 3 \rangle$ is maximal in $\mathbb{Z}$.

Lemma 1.2.2. *Let p be a prime in $\mathbb{Z}$. Then $\langle p \rangle$ is is maximal.*

Proof. Suppose J is an ideal in R and $\langle p \rangle \subset J \subset R$. Suppose $a \in J$ but a is not in $\langle p \rangle$. Then since p is prime p does not divide a. Hence $a = pq + r$ for some quotient q and remainder r satisfying $0 < r < p$. Now $a - pq = r$ and $a, p \in J$ imply $r \in J$. But $\gcd(r, p) = 1$ since p is prime. Thus there exist integers x, y such that $xr + yp = 1$. Since $r, p \in J$ this means $1 \in J$ thus $J = R$ and we have proven $\langle p \rangle$ is maximal. □

A similar result holds for ideals in $F[x]$ where F is a field. If f is an irreducible polynomial over F then $\langle f \rangle$ is maximal in $F[x]$. We consider an example.

Example 1.2.3. *Is $\langle x^2 - 1 \rangle$ maximal in $F[x]$? In $F[x]$ we have $x^2 - 1 = (x-1)(x+1)$. Let $J = \langle x - 1 \rangle$. Now $\langle x^2 - 1 \rangle \subset J \subset F[x]$ so $\langle x^2 - 1 \rangle$ is not maximal. Is $\langle x^2 + 1 \rangle$ maximal? This time it depends on F. If $F = \mathbb{Q}$ then since $x^2 + 1$ is irreducible over $\mathbb{Q}$ then $\langle x^2 + 1 \rangle$ is maximal. If $F = \mathbb{C}$ then since $x^2 + 1 = (x - i)(x + i)$ the ideal $J = \langle x - i \rangle$ satisfies $\langle x^2 + 1 \rangle \subset J \subset \mathbb{C}[x]$ so $\langle x^2 + 1 \rangle$ is not maximal.*

1.3 Ideals in Quotient Rings

Consider the finite ring $R = \mathbb{Z}_2[x]/(x^3 + 1) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$. What are the ideals in R? Let $f = x^3 + 1 = (x+1)(x^2+x+1)$. Observe that $\gcd(f, x) = 1, \gcd(f, x+1) = x+1, \gcd(f, x^2) = 1, \gcd(f, x^2+1) = x+1, \gcd(f, x^2+x) = x+1, \gcd(f, x^2+x+1) = x^2+x+1$ thus the units in R are 1 and x and x^2. Thus if I is an ideal containing 1 or x or x^2 then $I = R$. We obtain the following non-trivial ideals in R.

$$\langle x+1 \rangle = \{0, x+1, x^2+1, x^2+x\}$$
$$\langle x^2+x+1 \rangle = \{0, x^2+x+1\}$$

We recall that a quotient ring R is a vector space. It turns out that ideals in R are subspaces of R. Let f be in $F[x]$ have $n = \deg f > 0$ and let $R = F[x]/f$. For $s \in F$ and $[a] \in R$ we defined scalar multiplication $s[a] = [sa] = [s][a]$ and saw that R is a vector space over F.

Theorem 1.3.1. *Let I be an ideal in the quotient ring $R = F[x]/f$. Then I is a subspace of R.*

Proof. We have already shown that an ideal is closed under addition. Let $s \in F$. Now $s \in R$ since F is the constant subfield of R. Property (iii) means I is closed under multiplication by elements of R. Hence I is closed under scalar multiplication. Finally, I is not empty since $0_R \in I$ thus I is a subspace of R. □

Since an ideal I in a quotient ring $R = F[x]/f$ is a subspace of R we would like to know the dimension of I over F and it will be useful to know a basis for I. Continuing with the previous example we have

ideal in $\mathbb{Z}_2[x]/(x^3+1)$	basis	dimension
$\{0\}$	$\{\ \}$	0
$\{0, x+1, x^2+1, x^2+x\}$	$\{x+1, x^2+1\}$	2
$\{0, x^2+x+1\}$	$\{x^2+x+1\}$	1
R	$\{1, x, x^2\}$	3

1.4 Ideals in Algebra

We end our introduction to ideals by showing where ideals arise in algebra. We first show how ideals are connected with ring homomorphisms. We then take a first look at ideals in polynomial rings with more than one variable and connect ideals with solving systems of polynomial equations. In section 2.14 we will see that the BCH error correcting codes are constructed from ideals in the quotient ring $\mathbb{Z}_p[x]/(x^n-1)$.

Let R and S be two commutative rings and let $\phi : R \to S$ be a ring homomorphism. So $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$ and we are interested in the case here ϕ is not bijective. We have the following basic properties.

Lemma 1.4.1. *Let a, b be in R.*

(i) $\phi(0_R) = 0_S$,

(ii) $\phi(-a) = -\phi(a)$ *and*

(ii) $\phi(a-b) = \phi(a) - \phi(b)$.

Proof. To prove (i) first note that $\phi(0) = \phi(0+0) = \phi(0)+\phi(0)$. Now $0_S = \phi(0)-\phi(0) = (\phi(0)+\phi(0))-\phi(0) = \phi(0)+(\phi(0)-\phi(0)) = \phi(0)$. To prove (ii) we have $\phi(a)+\phi(-a) = \phi(a+(-a)) = \phi(0) = 0$ so $\phi(-a)$ is the additive inverse of $\phi(a)$. To prove (iii) we have $\phi(a-b) = \phi(a+(-b)) = \phi(a)+\phi(-b) = \phi(a)+(-\phi(b))$ by (ii) which equals $\phi(a)-\phi(b)$. $\square$

Definition 1.4.2. *Let R and S be two commutative rings with $\phi : R \to S$ a homomorphism. Then the kernel of ϕ is*

$$ker(\phi) = \{a \in R : \phi(a) = 0_S\}$$

So the kernel is all elements of R that are mapped to 0_S. As an example let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be given by $\phi(a) = a \mod n$. So $ker(\phi)$ is all integers divisible by n which is the ideal $\langle n \rangle$. As a second example let F be a field and $a \in F$. Consider $\phi : F[x] \to F$ where $\phi(f) = f(a)$. Here $ker(\phi)$ is all polynomials with root a, that is, all polynomials divisible by $x-a$ hence $ker(\phi) = \langle x-a \rangle$.

Lemma 1.4.3. *Let $\phi : R \to S$ be a homomorphism. Then $ker(\phi)$ is an ideal in S.*

Proof. Suppose a and b are in $ker(\phi)$ so that $\phi(a) = 0$ and $\phi(b) = 0$. Since ϕ is a homomorphism by Lemma 1.2.2 says $\phi(0_R) = 0_S$ hence $0_R \in ker(\phi)$. Now $\phi(a - b) = \phi(a) - \phi(b) = 0 - 0 = 0$ hence $a - b \in \ker(\phi)$. Finally let r be in R. Then $\phi(rb) = \phi(r)\phi(b) = \phi(r) \cdot 0 = 0$. Thus rb is in $ker(\phi)$. □

Consider the system of polynomial equations $\{x^2 - y^2 = 1, xy = 1\}$ and suppose we want to find the solutions in $\mathbb{R}^2$ if any. Let $f_1 = x^2 - y^2 - 1$ and $f_2 = xy - 1$. Consider the ideal

$$I = \langle x^2 - y^2 - 1, xy - 1\rangle \text{ in } \mathbb{R}[x, y].$$

Our goal is to find simpler generators for the ideal. First the polynomial

$$f_3 = yf_1 - xf_2 = yx^2 - y^3 - y - (x^2y - x^2) = x - y^3 - y$$

is in I because $f_1, f_2 \in I$. So we have $I = \langle f_1, f_2, f_3\rangle$. Now consider the polynomial

$$f_4 = f_2 - yf_3 = xy - 1 - (xy - y^4 - y^2) = y^4 + y^2 - 1$$

which is also in I because $f_2, f_3 \in I$. We now have

$$I = \langle f_1, f_2, f_3, f_4\rangle.$$

It turns out that $\{f_1, f_2, f_3, f_4\}$ is a special kind of basis for I called a Gröbner basis for I and as such we can stop looking for more generators. But $f_4 = f_2 - yf_3 \Rightarrow f_2 = f_4 + yf_3$ so f_2 is a redundant generator so $I = \langle f_1, f_3, f_4\rangle$. With some extra work we can show that $f_1 = (y^2 + 1)f_3 + (y^3 + x + y)f_4$ thus $f_1 \in \langle f_3, f_4\rangle$ so that

$$I = \langle f_3, f_4\rangle = \langle x - y^3 - y, y^4 + y^2 - 1\rangle.$$

It turns out that the new basis $\{f_3, f_4\}$ for I is still a Gröbner basis for I. And the two systems of equations $\{f_1 = 0, f_2 = 0\}$ and $\{f_3 = 0, f_4 = 0\}$ have the same solutions in $\mathbb{R}^2$, because changing the generators of an ideal does not change the solutions of the corresponding system of equations. It is also clear now how to solve $\{f_3 = 0, f_4 = 0\}$. For $\{x - y^3 - y = 0, y^4 + y^2 - 1 = 0\}$ has 4 solutions for y, two real and two complex, and for each solution for y the equation $x = y^3 + y$ gives one solution for x.

Exercises

1. Which of the following are ideals
   (a) $\mathbb{Q}$ in $\mathbb{R}$
   (b) $\{0, 2, 4, 6\}$ in $\mathbb{Z}_8$
   (c) $\mathbb{Z}$ in $\mathbb{Z}[i]$
   (d) $\{0, 1\}$ in GF(4)

(e) $\{0, x^2+1\}$ in $R = \mathbb{Z}_2[x]/(x^4+1)$

2. Find a single generator for the following ideals.

   (a) $\langle 12, 20\rangle$ in $\mathbb{Z}$
   (b) $\langle 12, 21, 15\rangle$ in $\mathbb{Z}$
   (c) $\langle x^2, x^3\rangle$ in $\mathbb{Q}[x]$
   (d) $\langle x^2-1, x^3-1\rangle$ in $\mathbb{Q}[x]$

3. Let I and J be ideals in a commutative ring R.

   (a) Prove that $I \cap J$ is an ideal in R.
   (b) Show that $I \cup J$ is not an ideal in general.
   (c) Prove that $I + J$ is an ideal in R.
   (d) For $I = \langle x^2-1\rangle$ and $J = \langle x^2 - x\rangle$ find generators for $I \cap J$ and $I + J$.

4. Consider the ideal $I = \{f \in \mathbb{Q}[x] : f(i) = 0\}$ where $i^2 = -1$. Prove that I is an ideal in $\mathbb{Q}[x]$ and find a generator g for I. Hint: what is the minimal polynomial for i in $\mathbb{Q}[x]$? Repeat this exercise with $J = \{f \in \mathbb{C}[x] : f(i) = 0\}$.

5. Let F be a field. Prove that every ideal in $F[x]$ is of the form $\langle f\rangle$ for some $f \in F[x]$. Hint: use the same argument in the proof of Theorem 1.1.10.

6. Let $R = \mathbb{Z}_2/(x^2+1)$ and $S = \mathbb{Z}_2/(x^2+x+1)$. List all ideals in R and S.

7. (a) Show that $\langle 2\rangle = \langle 10\rangle$ in $\mathbb{Z}_{14}$
   (b) Show that $\langle i\rangle = \mathbb{Z}[i]$ where $i^2 = -1$
   (c) Show that $\langle a, b, a+b\rangle = \langle a, b\rangle$ in a commutative ring R
   (d) Show that $\langle ua\rangle = \langle a\rangle$ if u is a unit in R

8. Let $I = \langle f_1, f_2, ..., f_s\rangle$ and $J = \langle g_1, g_2, ..., g_t\rangle$ be two ideals in a commutative ring R. Prove that $f_i \in J$ for $1 \leq i \leq s$ and $g_i \in I$ for $1 \leq i \leq t$ implies $I = J$. Now use this to prove that $\langle x+y-1, x-y\rangle = \langle x-y, 2y-1\rangle$.

9. Let F be a field and let $f \in F[x]$ with $\deg f > 0$. Show that $\langle f\rangle$ is maximal in $F[x] \iff f$ is irreducible over F.

10. Which of the following ideals are maximal in the given ring? If not maximal, give an ideal J lying strictly between the given ideal and ring.

    (a) $\langle 4\rangle$ in $\mathbb{Z}$
    (b) $\langle -3\rangle$ in $\mathbb{Z}$
    (c) $\langle x\rangle$ in $\mathbb{Q}[x]$
    (d) $\langle x^3+1\rangle$ in $\mathbb{Q}[x]$