1 Homework 1

(1) Prove the ideal (3,x) is a maximal ideal in $\mathbb{Z}[x]$.

SOLUTION: Suppose we expand this ideal by including another generator polynomial, $P \notin (3, x)$. Write $P = n + x * Q$ with n an integer not divisible by 3 (if $3|n$ then $P \in (3, x)$ so we have not expanded the ideal) and Q is some polynomial. Then subtracting off a multiple of one generator from another does not change the ideal (analogous to row operations on a matrix not changing the row space), so in particular $(3, x, P) = (3, x, n)$. As n is not a multiple of 3, $\gcd(3, n) = 1$, so $1 \in (3, x, P)$ and thus $(3, x, P)$ is all of $\mathbb{Z}[x]$. Thus (3,x) is maximal.

(2) Prove that (3) and (x) are prime ideals in $\mathbb{Z}[x]$.

SOLUTION: If P and Q are polynomials, then the constant term of PQ is the product of the constant terms of P and Q. Thus, if $PQ \in (x)$ then the product of their constant terms is 0, and since $\mathbb{Z}$ is an integral domain, this means one of them has a constant term equal to 0, hence lies in (x). Thus (x) is prime.

If neither P or Q is in (3), then each has at least one coefficient which is not a multiple of 3. Suppose p_i and q_j are such coefficients with i and j each minimal (i.e. come from the lowest degree term of P and Q such that the coefficient is not a multiple of 3).

Consider the coefficient of x^{i+j} in PQ, it is given by

$$[p_0 q_{i+j} + \ldots + p_{i-1} q_{j+1}] + [p_i q_j] + [p_{i+1} q_{j-1} + \ldots + p_{i+j} q_0]$$

As each of $p_0, \ldots, p_{i-1}$ is divisible by 3 by assumption, the first piece is divisible by 3, and likewise each of $q_0, \ldots, q_{j-1}$ is divisible by 3 so the third piece is also divisible by 3. But the middle term is not divisible by 3 since neither p_i nor q_j is divisible by 3, so the coefficient of x^{i+j} in PQ is not divisible by 3, so PQ does not lie in (3). Thus (3) is prime.

(3) Prove that the kernel of $\psi : \mathbb{Z}[x] \to \mathbb{R}$ given by $\psi(f) = f(\sqrt(3))$ is a principal ideal and find a generator for this ideal.

Checking the additive and multiplicative properties for $ker(\psi)$ is trivial, so it is an ideal.

SOLUTION (I): Since every polynomial can be factored into linear factors over $\mathbb{C}$, any $P \in ker(\psi)$ has $x - \sqrt{3}$ as a factor. But this factor is not in $\mathbb{Z}[x]$, so P is also divisible by the other $\mathbb{Z}$-conjugates of this factor, which in this case are just $x + \sqrt{3}$. Thus P is divisible by $[x - sqrt3][x + \sqrt{3}] = x^2 - 3$ and hence this is a generator.

SOLUTION (II): Alternatively, since the minimal degree polynomial in $\mathbb{Z}[x]$ which annihilates $\sqrt{3}$ is $x^2 - 3$ which has leading coefficient a unit in the coefficient ring $\mathbb{Z}$, by the division algorithm write an arbitrary $P \in ker(\psi)$ as $P(x) = (x^2 - 3)Q(x) + R(x)$ with $R(x) = ax + b$. Plugging in $\sqrt{3}$ into both sides of this expression, we see that $R(\sqrt{3}) = 0$ so that $a\sqrt{3} + b = 0$ for some

integers a and b. But this is clearly impossible unless $a = b = 0$, so $R(x) = 0$ and P is therefore divisible by $x^2 - 3$ which is therefore a generator for the ideal.

(4) Determine whether the following are PIDs. If not, exhibit a nonprincipal ideal.

(a) $\mathbb{Z}[t]$

SOLUTION: This is not a PID, this was shown in Problem (1).

(b) $\mathbb{R}[x, y]$

SOLUTION: This is not a PID, the ideal (x,y) is not principal.

(c) $\mathbb{Z}[\sqrt{-5}]$

SOLUTION: Unlike the previous two examples, this ring is not a UFD. We use this fact to construct a nonprincipal ideal. Consider $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, all four of these factors can be checked to be irreducible. Then ideals such as $(2, 1 + \sqrt{-5})$ obtained by taking one irreducible factor from each factorization are nonprincipal ideals in this ring.

(5) Let $\mathbb{F}$ be a field and $\mathbb{F}[[z]]$ the ring of power series.

(a) Show that every element $A = \sum_{i=0}^{\infty} a_i z^i$ such that $a_0 \neq 0$ is a unit in $\mathbb{F}[[z]]$.

SOLUTION: We want to show that there is $B = \sum_{i=0}^{\infty} b_i z^i$ such that $AB = 1 + 0z + 0z^2 + \ldots$ The coefficient b_0 must therefore be a_0^{-1} which exists since a_0 is assumed to be a nonzero element in a field. Inductively, assume we have calculated $b_0, \ldots, b_{k-1}$. The coefficient of z^k in AB is given by:

$$\begin{aligned} 0 &= [z^k]AB \\ &= \sum_{i=0}^{k} a_i b_{k-i} \\ &= a_0 b_k + \sum_{i=1}^{k} a_i b_{k-i} \end{aligned}$$

Therefore $b_k = -a_0^{-1} \sum_{i=1}^{k} a_i b_{k-i}$ which expresses b_k in terms of things which are known, hence we can calculate all b_k and thus $B = A^{-1}$ exists.

(b) Show that every non-zero ideal of $\mathbb{F}[[z]]$ is of the form $z^n \mathbb{F}[[z]]$ for some n.

SOLUTION: Let $I = (f_1, f_2, \ldots, f_j)$ be an ideal in $\mathbb{F}[[z]]$. As each f_i has a leading nonzero coefficient we can write:

$$\begin{aligned} f_i &= c_{k(i)} z^{k(i)} + c_{k(i)+1} z^{k(i)+1} + \ldots \\ &= z^k(i)(c_{k(i)} + c_{k(i)+1} z + \ldots) \\ &= z^k(i) \cdot u_i \end{aligned}$$

u_i is a unit by (a). Thus $I = (z^{k(1)}, z^{k(2)}, \ldots, z^{k(j)}) = (z^{min(k(1),k(2),\ldots,k(j))})$ since each $z^{k(i)}$ is clearly a multiple of this latter generator.

(c) Show that $\mathbb{F}[[z]]$ is a PID.

SOLUTION: This follows from (5b).

2 Homework 2

(1) Prove $R[x][y] \cong R[x,y]$.

SOLUTION: Elements of $R[x][y]$ are polynomials in y with coefficients which are polynomials in x. Thus there is an obvious bijection between the two rings, namely $(x^n)y^m \leftrightarrow x^n y^m$. It is easy to check that adding or multiplying monomial terms $x^n y^m$ in $R[x,y]$ and then mapping to $R[x][y]$ gives the same result as mapping to $R[x][y]$ and then adding or multiplying the resulting monomials and likewise for the other direction. Since the monomials generate these rings and the bijection preserves addition and multiplication of monomials, it is an isomorphism.

(2) If I is an ideal in R, show $rad(I) = \{x \in R | x^n \in I \text{ for some } n\}$ is an ideal.

SOLUTION: Suppose $x, y \in rad(I)$ and $x^n, y^m \in I$. Then binomial expansion of $(x+y)^{n+m-1}$ shows that each term is either of degree at least n in x or degree at least m in y, hence $(x+y) \in rad(I)$. For the multiplicative property, $xr \in rad(I)$ since $(xr)^n = x^n r^n \in I$ since $x^n \in I$.

(3) Factor $1+3i$ in $\mathbb{Z}[i]$ and factor $(1+3i)$ into maximal ideals.

SOLUTION: In $\mathbb{Z}[i]$, $N(a+bi) = a^2+b^2$. $N(1+3i) = 10$, so if it factors into $(p+qi)\cdot(r+si)$ then $N(p+qi) = 2$ and $N(r+si) = 5$ and hence both factors (if they exist) are irreducible. Clearly $p, q = (\pm 1)$ and $r, s = (\pm 1, \pm 2)$ in some order and checking, one finds the solution $1+3i = [1+i][2+i]$ (and others in which the factors differ from these by units $\{\pm 1, \pm i\}$). As $\mathbb{Z}[i]$ is a PID, $(1+i)$ and $(2+i)$ are generated by irreducible elements, hence maximal ideals, and so give the required factorization.

(4a) Is 5 irreducible in $\mathbb{Z}[i]$?

SOLUTION: No. A quick check, aided by norms, shows $5 = [2+i]\cdot[2-i]$, neither of which is a unit.

(b) Is (7) a prime ideal in $\mathbb{Z}[i]$?

SOLUTION: Since there are no solutions to $x^2+y^2 = 7$ in the integers, using norms we quickly establish that 7 is irreducible. As $\mathbb{Z}[i]$ is a UFD, irreducible$\leftrightarrow$ prime which implies (7) is prime.

(5a) Give an example of a maximal ideal in $\mathbb{R}[x,y]/(x^2+y^2+1)$

SOLUTION: Maximal ideals in a quotient ring R/I come from maximal ideals J such that $I \subset J \subset R$. In particular $(x, x^2+y^2+1) = (x, y^2+1)$ is one such maximal ideal. There are multiple ways to see this ideal is maximal. One way is to note that any $P \in \mathbb{R}[x,y]$ not in this ideal is equivalent to $ay+b$ for some $a, b \in \mathbb{R}$. To see this, subtract a multiple of x from P to leave a polynomial in y; then long divide this polynomial by y^2+1 to obtain a linear remainder $ay+b$ which, by construction, differs from P by a multiple of x plus a multiple of y^2+1. Thus, $(x, y^2+1, P) = (x, y^2+1, ay+b)$ and it can be checked from

here that this ideal therefore contains a constant, hence is the whole ring. Thus $(x, y^2 + 1)$ is maximal.

Alternatively, look at the quotient ring $\mathbb{R}[x, y]/(x, y^2 + 1) \cong \mathbb{R}[y]/(y^2 + 1)$. This latter ring is isomorphic to $\mathbb{C}$ since it is obtained by adjoining an element y to $\mathbb{R}$ such that $y^2 + 1 = 0$; i.e. y behaves like $\sqrt{-1}$. Since $\mathbb{C}$ is a field, we conclude $(x, y^2 + 1)$ is maximal.

(b) Show $(x^2 + y^2 + 1)$ is prime.

SOLUTION: Specializing at $y = 1$ gives $x^2 + 2$ which is irreducible in $\mathbb{R}[x]$, thus $x^2 + y^2 + 1$ is irreducible in $\mathbb{R}[x, y]$. Since $\mathbb{R}[x, y]$ is a UFD, principal ideals generated by irreducible elements are prime ideals, so $(x^2 + y^2 + 1)$ is a prime ideal.

3 Homework 3

(1) Show that the units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.

SOLUTION: It is easy to check these are the only elements of $\mathbb{Z}[i]$ with norm 1, hence are the only units.

(2) Let $f(x) = \sum_{i=0}^{d} a_i x^i \in R[x]$ such that $a_d \in R^\times$. Show that for any $g(x) \in R[x]$, there are unique $q(x)$ and $r(x)$ such that $g(x) = f(x)q(x) + r(x)$ and $deg(r) < deg(f)$.

SOLUTION: Apply the division algorithm to divide g by f; the successive terms of $q(x)$ are calculated by dividing $a_d x^d$ into the highest remaining term at each step. As a_d is a unit, this is always possible, hence the division algorithm gives a unique quotient. Uniqueness of $r(x)$ follows from uniqueness of $q(x)$.

(3) Let X_n be the $n \times n$ matrix whose (i,j)-entry is $x_{i,j}$. Show $det(X_n)$ is irreducible in $\mathbb{C}[x_{i,j}]_{1 \leq i,j \leq n}$.

SOLUTION: Since the determinant is linear in rows, no monomial term of $det(X_n)$ contains a subfactor of the form $x_{i,j}^2$ or $x_{i,j}x_{i,k}$. Suppose $det(X_n) = PQ$. Write $P = (x_{1,1}a_{1,1} + b_{1,1})$ and $Q = (x_{1,1}c_{1,1} + d_{1,1})$ with $a_{1,1}$, $b_{1,1}$, $c_{1,1}$ and $d_{1,1}$ polynomials in variables which do not involve $x_{1,1}$.

Since no terms of $det(X_n)$ are divisible by $x_{1,1}^2$, one of $a_{1,1}$ or $c_{1,1}$ is zero (but not both since there are terms of $det(X_n)$ which contain $x_{1,1}$). WLOG P contains $x_{1,1}$ as part of its terms. Now, for each k, rewrite $Q = (x_{1,k}c_{1,k} + d_{1,k})$, then $c_{1,k} = 0$ for all k by the same logic as above. Hence, all $x_{1,k}$ terms appear in P for all k. Using similar logic shows that all elements $x_{j,k}$ appear only in the same factor as $x_{1,k}$, but as this term appears in P, all variables only appear in P, hence Q is a unit and $det(X_n)$ is irreducible.

(4a) Suppose $s \in R$ is not nilpotent. Show that among all ideals which do not contain some power of s there is a maximal such ideal P containing all the others.

SOLUTION: Letting P be the union of all such ideals, it is clear P does not contain any power of s, while any larger ideal containing P must contain some power of s (otherwise it would be contained in P by construction, a contradiction), so we can apply Zorn's Lemma to conclude P is maximal.

(b) Let $I = \{x \in R | x \cdot s^n \in P \text{ for some } n\}$. Show I is an ideal not containing s.

SOLUTION: If $x, y \in I$ such that $x \cdot s^m, y \cdot s^n \in P$, then $(x+y) \cdot s^{max(m,n)} \in P$ so $x + y \in I$. If $r \in R$ is arbitrary, then $xr \cdot s^m = x \cdot s^m \cdot r \in P$ so $xr \in I$ and I is an ideal.

(c) Conclude $I = P$.

SOLUTION: No power of s can be in I since otherwise one would have $s^m \in P$ for some m. Thus $I \subseteq P$. On the other hand, every element of P is clearly in I, so $I = P$.

(d) Show P is prime.

SOLUTION: Suppose P is not prime and $u, v \notin P$ such that $uv \in P$. Consider the ideals (u, P) generated by u and all elements of P and (v, P) defined similarly. As $P \subset (u, P)$, $s^m \in (u, P)$ for some m and similarly $s^n \in (v, P)$ for some n. Therefore $s^m = r_1 u + p_1$ and $s^n = r_2 v + p_2$ for some $r_1, r_2 \in R$ and $p_1, p_2 \in P$. Thus:

$$s^{n+m} = r_1 r_2 uv + r_1 p_1 u + r_2 p_1 v + p_1 p_2$$

Now as $uv \in P$, every term on the right side is in P, hence $s^{n+m} \in P$, a contradiction. Thus P is prime.

(e) Let $rad(R)$ be the ideal of all nilpotent elements of R. Show $rad(R)$ is the intersection of all prime ideals of R.

SOLUTION: It is easy to check that rad(R) is an ideal. If $r \in rad(R)$ and P is a prime ideal then $r^n = 0 \in P$ so at least one of r or $r^n n - 1$ is in P. But if $r^{n-1} \in P$ then either r^{n-2} or r is in P, and repeating this argument, we conclude $r \in P$. Thus $rad(R)$ is contained in the intersection of all prime ideals. On the other hand, suppose p is in the intersection of all prime ideals of R but p is not nilpotent.

(5a) Show $\mathbb{Q}[\sqrt{2}]$ is a field and $dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}] = 2$.

SOLUTION: It is easy to check that the inverse of $a + b\sqrt{2}$ is $\frac{a-b\sqrt{2}}{a^2-2b^2}$. The denominator cannot be zero since otherwise $\sqrt{2} = \frac{a}{b}$, a contradiction since $\sqrt{2}$ is irrational. It is also easy to see that any element of $\mathbb{Q}[\sqrt{2}]$ can be written as $a + b\sqrt{2}$ with a, b rational, so that a $\mathbb{Q}$-basis for $\mathbb{Q}[\sqrt{2}]$ is $(1, \sqrt{2})$, hence this ring is 2-dimensional over $\mathbb{Q}$.

(b) Show $\mathbb{Q}[\sqrt{2}]$ is the fraction field of $\mathbb{Z}[\sqrt{2}]$.

SOLUTION: From (a) we know that any ratio of elements of $\mathbb{Z}[\sqrt{2}]$, say $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ can be written as $\frac{p}{q} + \frac{r}{s}\sqrt{2}$, so the fraction field of $\mathbb{Z}[\sqrt{2}]$ is contained in $\mathbb{Q}[\sqrt{2}]$. On the other hand, given $\frac{p}{q} + \frac{r}{s}\sqrt{2} \in \frac{Q}{[}\sqrt{2}]$, we can write it as $\frac{ps+rq\sqrt{2}}{qs}$ which shows that it is a ratio of elements of $\mathbb{Z}[\sqrt{2}]$. Thus $\mathbb{Q}[\sqrt{2}]$ equals the field of fractions of $\mathbb{Z}[sqrt2]$.

(c) Show $(\mathbb{Z}[\sqrt{2}]^{\times}$ is equal to the group generated by the units -1 and $1+\sqrt{2}$.

SOLUTION:

4 Extra Stuff

4.1 Norms and Factoring

For problems (3) and (4) in HW2, we introduce the concept of a norm function, which is useful for factoring in algebraic rings over the integers, the most common example being rings of the form $\mathbb{Z}[\sqrt{d}]$. Consider the effect of multiplication by a fixed element $a + b\sqrt{d}$. Treating an arbitrary $u + v\sqrt{d}$ as a column vector, the matrix corresponding to multiplication by $a + b\sqrt{d}$ is given by:

$$M(a + b\sqrt{d}) := \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

It is easy to check that this gives an injective homomorphism of $\mathbb{Z}[\sqrt{d}]$ into $Mat_{2\times 2}(\mathbb{R})$; so we have a matrix representation of this ring. Now the determinant of $M(a+b\sqrt{d})$ is $a^2 - db^2$; this number is defined to be the norm $N(a+b\sqrt{d})$. From properties of determinants, if $a+b\sqrt{d} = [p+q\sqrt{d}]\cdot[r+s\sqrt{d}]$ then $N(a+b\sqrt{d}) = N(p+\sqrt{d})N(r+s\sqrt{d})$. Thus the norm is a multiplicative (but not additive) homomorphism $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$.

An element of the ring such that $N(a+b\sqrt{d}) = \pm 1$ (i.e. the norm is a unit in the base ring $\mathbb{Z}$) is a unit in $\mathbb{Z}[\sqrt{d}]$ since it can easily be checked that its inverse is $\frac{[a-b\sqrt{d}]}{N(a+b\sqrt{d})}$ which is clearly an element of $\mathbb{Z}[\sqrt{d}]$. This observation further implies that if $N(a+b\sqrt{d})$ is prime in $\mathbb{Z}$ then $a+b\sqrt{d}$ must be irreducible in $\mathbb{Z}[\sqrt{d}]$.

4.2 Specialization

The concept of specialization is useful in determining when multivariable polynomials factor and in showing that they do not factor. The idea is that replacing a variable by a number, we do not lose factorizability, (although we may gain factorizability in the specialization when none exists in the original polynomial). For example, suppose x^2+y^2 factors as $P(x,y)Q(x,y)$ in $\mathbb{Q}[x,y]$. Then setting $y=1$ for example, it must still factor: $x^2+1 = P(x,1)Q(x,1)$. But as x^2+1 is irreducible in $\mathbb{Q}[x]$, we conclude the original polynomial was irreducible in $\mathbb{Q}[x,y]$ as well. On the other hand, since x^2+1 is reducible in $\mathbb{C}[x]$, we cannot conclude from specialization that x^2+y^2 is irreducible in $\mathbb{C}[x,y]$, and indeed it is not: $x^2+y^2 = (x+iy)(x-iy)$. On the other hand, x^2+y^2+c is irreducible in $\mathbb{C}[x,y]$ for $c \neq 0$, but any specialization of y always factors in $\mathbb{C}[x]$ (by the fundamental theorem of algebra), so factorizations in the specialization need not come from a factorization of the original polynomial.