Assignment III

Commutative Algebra, Math 6150

Kearnes 12:00

Nicholas Praterelli, John Tuley & Zachary Strider McGregor-Dorsey

Wednesday, Sept. 23, 2009

Problem #2

(a) Suppose that the commutative ring R is a UFD. Then a prime ideal in R is generated by some set of irreducible elements.

(b) Suppose that $R = S[x]$ where S is a PID. Then any prime ideal of R is generated by at most two irreducible elements. Further, if a prime ideal I requires two irreducible generators, then it has the form $I = (p, f(x))$ where p is prime in S and $f(x)$ is a monic polynomial in $S[x]$ that is irreducible mod p.

(c) Sketch the ordered set of primes of $S[x]$ under inclusion to the best of your ability. How long can a chain be?

Answer.

(a): Let P be a prime ideal, and let T be the set of all irreducible elements contained in P, together with 0. We claim that P is generated by T, proving our proposition. Clearly, the ideal (T) is contained in P since T, so we only need to show P is contained in (T).

Suppose $a \in P$. If $a = 0$, we are done, because $0 \in T$ by construction. Otherwise, we use that R is a UFD to write $a = q_1 q_2 \cdots q_n$ where each q_i is an irreducible element. We note here that if any of the q_i are in P, then that $q_i \in T$ by construction. We immediately have $a \in (T)$ by definition of ideal. We only need that one of the q_i is in P.

Since P is a prime ideal, we must have either $q_1 q_2 \cdots q_{n-1}$ or q_n in P. If $q_n \in P$, we are done. If not, $q_1 q_2 \cdots q_{n-1}$ is in P, so we again use the primality of P and find that either $q_1 q_2 \cdots q_{n-2}$ or q_{n-1} is in P. If the latter, we are again done. If the former, we apply this process once again. Because n is finite, we eventually find a q_i in P as needed.

Because a was chosen arbitrarily, we have that $P \subseteq (T)$, completing the proof. [DF04]

(b): Recall from general algebra that $R = S[x]$ is a UFD whenever S is a PID (or a UFD, for that matter).

Let P be a prime ideal of $R = S[x]$. We claim that $P \cap S$ is a prime ideal of S. Note that $P \cap S$ is exactly the constant polynomials contained in P. Also, it's clearly an ideal of S since $S \subseteq R$ and the sum and product of constant polynomials is again a constant polynomial.

Suppose $a(x) = b(x)c(x)$ is in $P \cap S$. Because S is a PID and hence an integral domain, the product of two polynomials in $S[x]$ has degree equal to sum of the degrees of the two polynomials. Thus, as degrees are nonnegative and the degree of $a(x)$ is 0, so must be the degrees of $b(x)$ and $c(x)$, i.e. they are constant polynomials. By the primality of P, either $b(x)$ or $c(x)$ is in P, say $b(x)$. Therefore $b(x) \in P \cap S$, as needed for primality.

Because S is a PID, there is an element p that generates the ideal $P \cap S$. Further, p is an irreducible (equivalently, prime) element, since $P \cap S$ is a prime ideal, or p is zero.

Suppose that p is not zero. Note that p is irreducible in R for the same reasoning as above, i.e. any two elements of R whose product is constant must also be constant. From part a), we know that there is some set T of irreducibles that generate P. From the proof, we know we can assume that $p \in T$.

Because $p \in P$, we know that $pR \subseteq P$. Thus we can examine the quotient P/pR in the ring R/pR. Because P is prime in R, we know that P/pR is also prime (possibly 0) in R/pR by the one-to-one correspondence between ideals of R containing pR and ideals of R/pR [DF04, Corollary 13 p 255]. If P/pR is 0, we are done, because the $P = pR$ and generated by a single element. Assume P/pR is not trivial.

We will show that R/pR is a PID. If that is the case, the ideal P/pR is generated by a single prime (irreducible) element, say $f(x) + pR$. The correspondence theorem then states that P is the ideal generated by p and $f(x)$.

Because S is a PID and p is not zero, we know that pS is in fact a maximal ideal of S [DF04, Proposition 7 p 280], so S/pS is a field. Thus $S/pS[x]$ is a PID [DF04, p 281]. It is well known that $S/pS[x]$ is isomorphic to $S[x]/pS[x] = R/pR$.

Finally, we note that we can assume that $f(x)$ is a monic polynomial. If it is not, let c be its leading coefficient, which is clearly nonzero. Its image under the natural map from S to S/pS is invertible because S/pS is a field. The surjectivity of the natural map guarantees that there is an $a \in S$ which is sent to that inverse. Note that $af(x) + pR$ generates the same ideal in R/pR as $f(x) + pR$ does because we are simply multiplying by a unit. Because $ac = 1 \pmod p$, the polynomial $g(x)$ which is identical to $af(x)$ except at the leading coefficient which is set to 1 is equivalent to $af(x) \bmod p$.

Thus $g(x)+pR$ generates the same ideal in R/pR as $af(x)+pR$ because they are in fact the same element in R/pR. (Note that the fact it generates a prime ideal implies $g(x)$ is prime and hence irreducible in R/pR, which immediately implies $g(x)$ is irreducible in R.) Thus the ideal generated by p and $g(x)$ must be same as that generated by p and $f(x)$, so we can replace f by g if need be.

We have shown that P is generated by p and $f(x)$, a monic polynomial irreducible mod p.

Now suppose the p is zero, i.e. that P contains no nonzero constant polynomials. Let f be an irreducible polynomial in P of minimal degree. The degree of f is not 0 since it is nonconstant. Let g be any other polynomial in P, also nonconstant. If we pass to the field of fractions of $\mathrm{Frac}(S)$, we know that f and g are also polynomials in $\mathrm{Frac}(S)[x]$. Because $\mathrm{Frac}(S)$ is a field, $\mathrm{Frac}(S)[x]$ is a Euclidean domain. Thus we can apply the Euclidean algorithm to get

$$g = fq + r$$

with $q, r \in \mathrm{Frac}(S)[x]$ and the degree of r less than that of f.

We then multiply by some nonzero element $s \in S$ that clears the denominators of all the coefficients in the polynomials q and r to get

$$sg = sfq + sr,$$

a statement now true in $S[x]$. (We could define s to be, simple, the product of all the denominators of all the coefficients that appear in q and r, so s exists.) Because f and g are in P, so must be $sg - (sq)f = sr$.

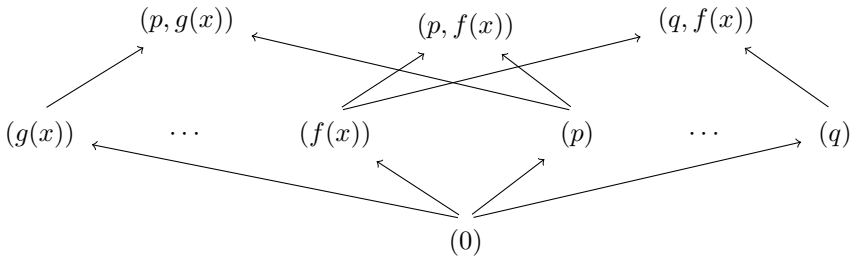
If r is a constant, then so is sr, which means $sr = 0$, the only constant in P. As we are in an integral domain and s is not zero, r must be.

If r is a polynomial of positive degree, then sr is of the same degree (again because S is an integral domain). The polynomial sr may not be irreducible, but R is a UFD, so we can write it as a product of irreducible factors. In the normal way (see the proof of (a)), the primality of P implies one of those irreducible factors is in P. But these factors have degree less than r which has degree less than f, contradicting the minimality of f.

So we have that r is zero. Thus $sg = sfq$. Now, the right hand side of the equation is in the ideal generated by f, since sq is in $S[x]$. Therefore $sg \in (f)$. But f is prime, so (f) is prime, giving us that either s or g is in (f). Clearly s is not, as s is a nonzero constant and f is not. Thus g must be. Since g was chosen arbitrarily, we get $P \subseteq (f)$, i.e. $P = (f)$.

(c): From the above, we know that any prime ideal P of $S[x]$ has one of the following forms:

- $P = (p)$ where p is a prime in S.
- $P = (f(x))$ where $f(x)$ is a prime and nonconstant in R.
- $P = (p, f(x))$ where p is a prime in S and $f(x)$ is a monic polynomial irreducible mod p



In this diagram, p, q are primes in S (hence are irreducible constant polynomials in R) and $f(x), g(x)$ are arbitrary nonconstant monic irreducible polynomials in R. Given each pair $p, f(x)$, we obtain a version of the central diamond in the diagram. For any other $g(x)$, p and $g(x)$ form another diamond with vertices (0), (p), $(g(x))$, and $(p, g(x))$; likewise, for any other prime q, we obtain a diamond with vertices (0), (q), $(f(x))$ and $(q, f(x))$. The longest chain length of nontrivial prime ideals is 2.

□

References

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., 2004.