POLYNOMIAL RINGS

COLTON GRAINGER (MATH 6130 ALGEBRA)

12. Assignment due 2018-12-12

12.1. **[1, No. 9.1.4].** *Given.* Let (x) and (x, y) be ideals in the ring of polynomials $\mathbf{Q}[x, y]$.

To prove.

i. (x) is prime and not maximal.
ii. (x, y) is prime and maximal.

Proof. We can obtain an isomorphic copy of any ring R from its polynomial ring R[x] either

- by taking the image of R[x] under the evaluate at 0 ring homomorphism, or
- by quotienting out the ideal generated by the indeterminate (x).

That $R \cong \mathrm{ev}_0\,(R[x])$ is apparent; we'll justify $R \cong R[x]/(x)$. Consider the homomorphism $\pi \circ \iota \colon R \to R[x]/(x)$, as in the following commutative diagram.

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[dr, "\pi \circ \iota"'] & R[x] \arrow[d, "\pi"] \\ & R[x]/(x) \end{tikzcd}$$

For all nonzero $a \in R$, in $R[x]$ the ideal (x) does not contain a. Whence $\ker(\pi \circ \iota) = 0$. Similarly, for each $r + (x) \in R[x]/(x)$, there's $r \in R$ such that $\pi(\iota(r)) = r + (x)$. So $\pi \circ \iota$ is ring isomorphism.

In particular, consider the field $\mathbf{Q}$ and the UFD $\mathbf{Q}[y]$:

i. $\mathbf{Q}[x, y]/(x) \cong \mathbf{Q}[y]$ is an entire ring, but not a field. Thus (x) is prime, but not maximal [1, Sec. 7.4].
ii. $\mathbf{Q}[x, y]/(x, y) \cong (\mathbf{Q}[x][y]/(y))/(x) \cong \mathbf{Q}[x]/(x) \cong \mathbf{Q}$ is a field. Thus (x, y) is maximal (so prime too). The isomorphism $\mathbf{Q}[x, y]/(x, y) \cong (\mathbf{Q}[x][y]/(y))/(x)$ follows from $(x, y) = (x) + (y)$. □

12.2. **[1, No. 9.1.10].** *Given.* Let R be the polynomial ring $\mathbf{Z}[x_1, x_2, x_3, \ldots]$, a UFD [1, Sec. 9.3]. Let $\overline{R}$ be the quotient ring $\mathbf{Z}[x_1, x_2, x_3, \ldots]/(x_1x_2, x_3x_4, x_5x_6, \ldots)$.

To prove. $\overline{R}$ contains infinitely many minimal prime ideals. We define a minimal prime ideal as "an ideal $\mathfrak{p}$ in a commutative unital ring R that's *prime* and does not strictly contain another prime ideal."[1]

Proof. We inject the set $2^{\mathbf{N}}$ of infinite coin flips into the set of minimal prime ideals in $\overline{R}$ via the function

$$\text{the sequence } (e_1, e_2, e_3, \ldots) \mapsto \text{ the ideal } (x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots).$$

It's routine to verify this function is an injection. We now focus to argue each ideal in the image is a minimal prime ideal.

Date: 2018-12-10.
Compiled: 2019-01-03.

[1] https://commalg.subwiki.org/wiki/Minimal_prime_ideal

- Observe $(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots) \supset (x_1x_2, x_3x_4, x_5x_6, \ldots)$. So

$$\overline{R}/(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots) \cong R/(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots).$$

  For each "coin flip", need indices to access "the complementary event". So define $\overline{e_n} = 0$ if $e_n = 1$, else $\overline{e_n} = 1$. By quotienting, we're just killing off the indeterminates whose indices are "hit" by our particular sequence of coin flips. So

$$R/(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots) \cong \mathbf{Z}[x_{1+\overline{e_1}}, x_{3+\overline{e_2}}, x_{5+\overline{e_3}}].$$

  Relabelling indices,

$$\mathbf{Z}[x_{1+\overline{e_1}}, x_{3+\overline{e_2}}, x_{5+\overline{e_3}}] \cong R.$$

  Stringing these isomorphisms together, we conclude that the ideal $(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots)$ is *prime* in $\overline{R}$ because the quotient $\overline{R}/(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots) \cong R$ is entire.

- Now consider any proper ideal $\mathfrak{a} \subsetneq (x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots)$. We can think of $\mathfrak{a}$ as a sequence of coin flips that forgets at least one outcome. So verify that

$$\mathfrak{a} \not\supset (x_1x_2, x_3x_4, x_5x_6, \ldots).$$

  In particular, there's some odd positive i for which the product $x_ix_{i+1} \notin \mathfrak{a}$ (one of the events forgotten!). Quotienting $\mathfrak{a}$ out of $\overline{R}$, the ring $\overline{R}/\mathfrak{a}$ has $\overline{x_i}$ and $\overline{x_{i+1}}$ as zero divisors. Therefore $\mathfrak{a}$ is not prime. We conclude $(x_{1+e_1}, x_{3+e_2}, x_{5+e_3}, \ldots)$ is a *minimal* prime ideal. □

12.3. **[1, No. 9.1.13].** *Given.* Let F be a field.

To prove. The rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(y^2 - x^2)$ are not isomorphic.

Proof. As F is a field, $F[y]$ is a Euclidean domain, hence $F[x, y]$ is a UFD. So the irreducible polynomials in $F[x, y]$ are exactly the prime polynomials. Now

- $y^2 - x^2 = (y - x)(y + x)$ is not prime, thus $F[x, y]/(y^2 - x^2)$ has zero divisors;
- $y^2 - x$ is irreducible,[2] so prime, thus $F[x, y]/(y^2 - x)$ is an entire ring.

Since the property of being an entire ring is invariant under ring isomorphism, the two quotients cannot be isomorphic. □

Lemma. Suppose F is a field. Let $f(x) \in F[x]$ be a polynomial of degree $n \geqslant 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. For each $\overline{g(x)}$ there's a unique polynomial $r(x)$ of degree strictly less than n such that $\overline{g(x)} = \overline{r(x)}$.

Proof. Let $f(x) \in F[x]$ as above, a nonconstant polynomial. Let $\overline{g(x)} \in F[x]/(f(x))$. There exists $g(x) \in F[x]$ which projects to $\overline{g(x)}$. Now $F[x]$ is a Euclidean domain (with a division algorithm that produces *unique* remainders), so divide $g(x)$ by $f(x)$ to obtain unique $a(x), r(x) \in F[x]$ such that

$$g(x) = a(x)f(x) + r(x) \quad \text{where} \quad 0 \leqslant \deg r < \deg f.$$

The difference $g(x) - r(x) \in (f(x))$, so in the quotient $\overline{g(x)} = \overline{r(x)}$. □

Knowing the lemma holds, we know each for polynomial $\overline{g(x)} \in F[x]/(f(x))$, there's a unique $r(x) \in F[x]$ such that $\overline{g(x)} = \overline{r(x)}$, where $\overline{r(x)}$ is in the span of the elements $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$. To see this span is minimal, consider that its vectors are pairwise orthogonal.

[2] Consider $-x + y^2$ as a polynomial in x with coefficients in $F[y]$. It's linear. Into what non-constant polynomials could it factor?

12.4. **[1, No. 9.2.2].** *Given.* Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geqslant 1$.

To prove. $F[x]/(f(x))$ has q^n elements.

Proof. We enumerate each distinct vector $\overline{r(x)}$ (of degree strictly less than n as above) in $F[x]/(f(x))$ by the coefficient of its kth degree term for $k = 0, \dots, n-1$. But each coefficient is in the finite field $\mathbf{F}_q$, so the number of distinct coefficients for $\overline{r(x)}$ is q^n. By lemma, $\overline{1}, \overline{x}, \dots, \overline{x^{n-1}}$ is a basis. By considering the distinct coefficients of $\overline{r(x)}$, we've taken exactly all distinct linear combinations of basis vectors. Since each of n basis vectors can be scaled with one of q scalars in the finite field $\mathbf{F}_q$, we conclude $|F[x]/(f(x))| = q^n$. □

12.5. **[1, No. 9.2.3].** *Given.* Let $f(x)$ be a polynomial in $F[x]$.

To prove. $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proof. We apply the hierarchy theorem in full force to exploit that $F[x]$ is a Euclidean domain. (⇒) Suppose that $F[x]/(f(x))$ is a field. Then $(f(x))$ is a maximal ideal. As $F[x]$ is an entire ring, $(f(x))$ is prime. Because $F[x]$ is a UFD, $f(x)$ is irreducible. (⇐) Suppose $f(x)$ is irreducible. Then as $F[x]$ is a Euclidean domain, $f(x)$ is prime. Now $(f(x))$ is a prime ideal in a PID, so $(f(x))$ is maximal. Therefore $F[x]/(f(x))$ is a field. □

12.6. **[1, No. 9.2.4].** *Given.* Let F be a finite field.

To prove. $F[x]$ contains infinitely many primes.

Proof by contradiction. Suppose $\{p_1(x), \dots, p_n(x)\}$ is the finite set of all prime polynomials in $F[x]$. Consider the nonconstant polynomial

$$f(x) = \prod_1^n p_i(x) + 1$$

in $F[x]$. Since none of prime ideals $(p_i(x))$ contain 1, neither do they contain $f(x)$. But $F[x]$ is a Euclidean domain, so a UFD, and we must have a representation of

$$f(x) = \prod_1^m q_j(x)$$

as a product of irreducible, thus prime, polynomials $q_j(x)$. By construction of $f(x)$,

$\{q_1(x), \dots, q_m(x)\}$ and $\{p_1(x), \dots, p_n(x)\}$ are disjoint.

Absurd!—$\{p_1(x), \dots, p_n(x)\}$ is supposed to be the exhaustive set of primes! □

12.7. **[1, No. 9.2.10].** *To find.* The greatest common divisor of $m(x) = x^3 + 4x^2 + x - 6$ and $n(x) = x^5 - 6x + 5$ in $\mathbf{Q}[x]$, expressed as a $\mathbf{Q}[x]$-linear combination of $m(x)$ and $n(x)$.

Demonstration. A GCD of $n(x)$ and $m(x)$ is $x - 1$. It's the last nonzero remainder in the extended Euclidean algorithm. In gruesome hard-coded detail (*feel free to skim to the next page*).

```
>>> R.<x> = PolynomialRing(QQ, sparse=True)
>>> # n.quo_rem(m) long divides n by m and returns (quotient, remainder)
>>> (x^5 - 6*x + 5).quo_rem(x^3 + 4*x^2 + x - 6)
(x^2 - 4*x + 15, -50*x^2 - 45*x + 95)
>>> (x^3 + 4*x^2 + x - 6).quo_rem(-50*x^2 - 45*x + 95)
(-1/50*x - 31/500, 11/100*x - 11/100)
>>> (-50*x^2 - 45*x + 95).quo_rem(11/100*x - 11/100)
(-5000/11*x - 9500/11, 0)
```

We also want Bézout coefficients, to see that $x-1$ is a linear combination of $n(x)$ and $m(x)$. Here's an imperative implementation[3] of the extended Euclidean algorithm that records the desired coefficients.

```
>>> def extgcd(n,m):
>>>
>>>     """a wrapper around SAGE to compute a GCD and Bézout coefficients"""
>>>
>>>     # initialize remainder and Bézout coeff arrays
>>>     r = []; s = [1,0]; t = [0,1]
>>>
>>>     # we assume deg(n) >= deg(m)
>>>     r.append(n)
>>>     r.append(m)
>>>
>>>     # while the last remainder is nonzero
>>>     while r[-1] != 0:
>>>
>>>         # long divide
>>>         (quo,rem) = r[-2].quo_rem(r[-1])
>>>
>>>         # append remainder and latest Bézout coeffs
>>>         r.append(rem)
>>>         s.append(s[-2] - quo*s[-1])
>>>         t.append(t[-2] - quo*t[-1])
>>>
>>>     # second to last remainder and coeffs
>>>     return r[-2], s[-2], t[-2]
```

Why is this procedure meaningful? Because we can quickly find a polynomial $n(x)s(x) + m(x)t(x)$ that's an associate of $x - 1 \in \text{GCD}\{n(x), m(x)\}$, i.e., we may find "scalars" s and t to form linear combination of $n(x)$ and $m(x)$ that generates the ideal $(x - 1)$.

```
>>> n = x^5 - 6*x + 5
>>> m = x^3 + 4*x^2 + x - 6
>>> ### extgcd returns a 3-tuple
>>> (gcd, s, t) = extgcd(n,m)
>>> print(gcd, s, t)

(11/100*x - 11/100, 1/50*x + 31/500, -1/50*x^3 + 9/500*x^2 - 13/250*x + 7/100)

>>> n*s + m*t == gcd

True
```

12.8. **[1, No. 9.3.3].** *Given.* Let F be a field.

To prove. The set R of polynomials in $F[x]$ whose coefficient of x is equal to 0 is a subring of $F[x]$. Moreover, R is not a UFD.

[3] See https://doc.sagemath.org/html/en/reference/polynomial_rings/sage/rings/polynomial/polynomial_element_generic.html, https://en.wikipedia.org/wiki/Polynomial_greatest_common_divisor.

Proof. Say $r(x), s(x) \in R$. Subtracting like powers, $r(x) - s(x) \in R$. Hence $(R, +)$ is an abelian subgroup of $F[x]$. Say that $r(x) = \sum_{i=0}^{n} r_i x^i$ and $s(x) = \sum_{j=0}^{m} s_j x^j$. Then

$$r(x)s(x) = \sum_{k=0}^{mn} \sum_{i+j=k} r_i s_j x^k = r_0 s_0 + \underbrace{r_1 s_0 + r_0 s_1}_{\text{just } 0} x + \text{ higher order terms } \in R.$$

We conclude $(R, \cdot)$ is a semigroup under the associative multiplication inherited from $F[x]$. (We could also say $1 \in R$.) So R is a subring of $F[x]$.

Now consider $x^6 \in R$. Observe $(x^3)^2 = (x^2)^3 = x^6$. We'll show x^2 and x^3 are irreducible in R. Consider the possible factorizations, up to associates, of x^2 and x^3:

- $x^3 = x^0 x^3 = x^2 x^1$. The first factorization is not into irreducibles and the later is not in R.
- $x^2 = x^0 x^2 = x^2 x^1$. Dido.

We conclude that x^6 has two distinct factorizations; therefore R is not a UFD. □

12.9. **[1, No. 9.4.7].** *Given.* The ring of polynomials $\mathbf{R}[x]$ and the ideal generated by $x^2 + 1$.

To prove. $\mathbf{R}[x]/(x^2 + 1)$ is a field that's isomorphic to the complex numbers.

Proof. We exhibit an isomorphism. Define $\varphi\colon \mathbf{C} \to \mathbf{R}[x]/(x^2 + 1)$ by $a + bi \mapsto \overline{a} + \overline{bx}$ for all $a, b \in \mathbf{R}$.

- φ is a well defined ring homomorphism. Additivity is clear, $\varphi(\vec{u}) + \varphi(\vec{v}) = \varphi(\vec{u} + \vec{v})$. For multiplicativity, note in $\overline{\mathbf{R}[x]}$ $\overline{0} = \overline{bd(x^2 + 1)}$. Exploit this!
$$\begin{aligned}\varphi(a + bi)\varphi(c + di) &= \overline{ac} + \overline{adx} + \overline{bcx} + \overline{bdx^2}\\ &= \overline{ac - bd} + \overline{(ad + bc)x}\\ &= \varphi((a + bi)(c + di)).\end{aligned}$$
- φ is injective. For say (real numbers) $a \neq c$ or $b \neq d$. Then $\varphi(a + bi) = \overline{a} + \overline{bx} \neq \overline{c} + \overline{dx} = \varphi(c + di)$.
- φ is surjective by lemma. Recall for each $\overline{g(x)} \in R[x]/(x^2 + 1)$ there's a unique $r(x)$ of degree less than 2 such that $\overline{r(x)} = \overline{g(x)}$. Whence $\{\overline{1}, \overline{x}\}$ is a basis for the vector space $\mathbf{R}[x]/(x^2 + 1)$ over $\mathbf{R}$. φ is an $\mathbf{R}$-linear map and takes $1 \mapsto \overline{1}$ and $i \mapsto \overline{x}$.

We conclude the field of complex numbers $\mathbf{C}$ is the extension of $\mathbf{R}$ in which the polynomial $x^2 + 1$ has a root. □

12.10. **[1, No. 9.4.12].** *Given.* The ring of polynomials $\mathbf{Z}[x]$ and the polynomial $x^{n-1} + x^{n-2} + \cdots + x + 1$.

To prove. $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible in $\mathbf{Z}[x]$ if and only if n is a prime.

Proof.[4] ($\Rightarrow$) Suppose p is prime. Then $\sum_{i=0}^{p-1} x^i = \Phi_p(x)$ is the pth cyclotomic polynomial. Consider the transformation

$$\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

We see $\Phi_p(x + 1)$ is a monic polynomial, with coefficients

$$\frac{p!}{(p - k)!k!} \quad \text{divisible by } p \text{ for} \quad k \in \{1, \ldots, p - 1\}.$$

Further, $p^2 \nmid p$, the constant coefficient of $\Phi_p(x + 1)$. Applying Eisenstein's criterion, we conclude $\Phi_p(x + 1)$ (hence $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$) is irreducible over $\mathbf{Z}[x]$.

[4] I consulted: https://web.archive.org/web/20150524162238/https://crazyproject.wordpress.com/2011/01/03/prove-that-a-given-family-of-polynomials-is-reducible-over-zz/. The ideal to massage the convolution in the case that n is composite was not my own. The write-up was entirely my own.

($\Leftarrow$) Suppose n is composite. Consider $\sum_{i=0}^{n-1} x^i$. We'll reshape the indices of our sum from an $n \times 1$ vector down into a $d \times q$ matrix, where $n = dq$ for integers $d, q > 1$. A naive attempt would be to write $\sum_{i=0}^{d-1} \sum_{j=0}^{q-1} x^{ij}$. One should verify ij is a poor choice of exponent given that we're trying to establish a one-to-one correspondence between $\{0, \dots, d-1\} \times \{0, \dots, q-1\}$ and $\{0, \dots, n-1\}$. Rather, we rely on the (non-negative and therefore unique) division algorithm in $\mathbf{Z}$ to represent each $N \in \{0, \dots, n-1\}$ *uniquely* as $N = di + j$ where $0 \leqslant j < d$. The range of the index j forces $0 \leqslant i \leqslant \left\lfloor \frac{n-1}{q} \right\rfloor = d - 1$.

By order considerations, the injection $(i, j) \mapsto di + j$ is a bijection between $\{0, \dots, d-1\} \times \{0, \dots, q-1\}$ and $\{0, \dots, n-1\}$. We find here a reduction of $1 + x + \ldots + x^{n-1}$ into nonconstant polynomials:

$$\sum_{i=0}^{n-1} x^i = \sum_{i=0}^{d-1} \sum_{j=0}^{q-1} x^{di+j} = \left(\sum_{i=0}^{d-1} x^{di} \right) \left(\sum_{j=0}^{q-1} x^j \right). \square$$

12.11. **[1, No. 9.4.16].** *Given.* Let F be a field and let $a(x)$ be a polynomial of degree n in $F[x]$. The polynomial $b(x) = x^n a(1/x)$ is called the reverse of $a(x)$.

To demonstrate. (a) Describe the coefficients of b in terms of the coefficients of a. (b) a is irreducible if and only if b is irreducible.

Demonstration.

(a) Both $a(x)$ and its reverse $b(x)$ have the same degree, the same number of coefficients, and are elements of the same polynomial ring $F[x]$. Explicitly, when $a(x) = \sum_1^n a_i$, $b_j = a_{n-j}$ and $b(x) = \sum_1^n b_j$.

(b) Say that $a(x)$ is reducible into $d(x)q(x)$, nonconstant polynomials in $F[x]$ of degree m and ℓ respectively. Now $d(x)$ and $q(x)$ are nonconstant if and only if $x^m d(1/x)$ and $x^\ell q(1/x)$ are nonconstant (in $F[x]$), which occurs if and only if the reverse $x^{m\ell} a(1/x) = x^m d(1/x) x^\ell q(1/x)$ is reducible into nonconstant polynomials in $F[x]$. $\square$

12.12. **A variant of Eisenstein's Criterion [1, No. 9.4.17].** *Given.* Let $\mathfrak{p}$ be a prime ideal in the Unique Factorization Domain R and let $a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$, $n \geqslant 1$. Suppose $a_n \notin \mathfrak{p}$, $a_{n-1}, \dots, a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$.

To prove. $a(x)$ is irreducible in $F[x]$, where F is the quotient field of R.

Proof. Once we've established that $a(x)$ is irreducible in $R[x]$, by (the contrapositive to) Gauss' lemma, $a(x)$ will be irreducible in $F[x]$. So let R and $\mathfrak{p}$ be as above. Let $a(x) \in R[x]$ with coefficients as above. To argue that $a(x)$ is irreducible in $R[x]$, we suppose it's not and approach a contradiction. So let $a(x) = b(x)c(x)$ for nonconstant polynomials $b(x), c(x)$ in $R[x]$. Consider residues under the reduction homomorphism $R[x] \to R/\mathfrak{p}[x]$. The equation

$$a(x) = b(x)c(x) \quad \text{in } R[x] \text{ reduces modulo } \mathfrak{p} \text{ to} \quad a_n x^n + \mathfrak{p} = \left(\sum (b_i + \mathfrak{p}) x^i \right) \left(\sum (c_j + \mathfrak{p}) x^j \right).$$

Because

- $R/\mathfrak{p}$ is an integral domain[5] and
- the reduced polynomials satisfy $\deg \overline{a(x)} = \deg \overline{b(x)} + \deg \overline{c(x)}$

it must be that *both residues* $\overline{b(x)}$ and $\overline{c(x)}$ have zero for their constant terms. That is, in $R/\mathfrak{p}$, we have $b_0 + \mathfrak{p} = c_0 + \mathfrak{p} = \mathfrak{p}$. Pulling back to R, $a_0 = b_0 c_0 \in \mathfrak{p}^2$—a contradiction! Our assumption that $a(x)$ is reducible must be faulty. $\square$

[5] I don't believe it's a UFD, but I could be wrong. In the case that $R = \mathbf{Z}$, reduction mod a prime p *does* produce a UFD $\mathbf{F}_p$.

References

[1] D. Dummit and R. Foote, *Abstract algebra*. Prentice Hall, 2004.