RINGS OF FRACTIONS, THE CRT, EUCLIDEAN DOMAINS, PIDS, UFDS

COLTON GRAINGER (MATH 6130 ALGEBRA)

From Lang [1, Sec. II.1]:

> Most of the rings without zero divisors which we consider will be commutative. In view of this, we define a ring A to be **entire** if $1 \neq 0$, if A is commutative, and if there are no zero divisors in the ring. (Entire rings are also called **integral domains**. However, linguistically, I feel the need for an adjective. "Integral" would do, except that in English "integral" has been used for "integral over a ring". In French, as in English, two words exist with similar roots: "integral" and "entire". The French have used both words. Why not do the same in English? There is a slight psychological impediment, in that it would have been better if the use of "integral" and "entire" were reversed to fit the long-standing French use. I don't know what to do about this.)

11. Assignment due 2018-12-05

11.1. **[2, No. 7.5.4].** *Given.* A subfield $\mathbf{F}$ of $\mathbf{R}$.

To prove. $\mathbf{F}$ contain $\mathbf{Q}$.

Proof. The entire ring of integers $\mathbf{Z}$ has field of fractions $\mathbf{Q}$. If a field $\mathbf{F}$ contains a copy of $\mathbf{Z}$, then the subfield of $\mathbf{F}$ generated by $\iota(\mathbf{Z})$ is isomorphic to $\mathbf{Q}$. For let's define the injection on generators

$$\iota \colon \mathbf{Z} \to \mathbf{F} \quad \text{such that } 1 \mapsto 1_{\mathbf{F}}.$$

Since $\mathbf{R}$ has characteristic 0, $\mathbf{F}$ does too. That is, ι has trivial kernel $0\mathbf{Z}$. We identify $\mathbf{Z} \hookrightarrow \mathbf{F}$. Because the field of fractions $\mathbf{Q}$ is the smallest field containing $\mathbf{Z}$, we must have $\mathbf{F} \supset \mathbf{Q}$. □

11.2. **[2, No. 7.5.5].** *Given.* Let F be a field, let $F[[x]]$ be the ring of formal power series in the indeterminate x with coefficients in F.

To prove.

i. The ring of fractions of $F[[x]]$ is the ring $F((x))$ of formal Laurent series.
ii. The field of fractions of the power series ring $\mathbf{Z}[[x]]$ is *properly* contained in the field of Laurent series $\mathbf{Q}((x))$

Proof.

i. (Notation: suppose for $\sum a_n x^n \in F[[x]]$, we define a_i for *all* $i \in \mathbf{Z}$ by letting $a_k = 0$ when $k < 0$.) Because F is an entire ring, if $\sum a_n x^n, \sum b_n x^n \in F[[x]] \setminus \{0\}$, then

$$\sum a_n x^n \sum b_n x^n = \sum_{n\geq 0} \left(\sum_{i+j=n} a_i b_j x^n \right) = \underbrace{a_k b_\ell \cdot}_{\text{first nonzero coefficients}} x^{k+\ell} + \sum_{n>k+\ell} \left(\sum_{i+j=n} a_i b_j x^n \right).$$

So $F[[x]]$ is entire, and therefore has a *field* of fractions.

Date: 2018-11-28.
Compiled: 2018-12-05.

Now to argue that this field of fractions is $F((x))$. We need to demonstrate for all $\sum a_n x^n \in F[[x]] \setminus \{0\}$, there exists some $(\sum a_n x^n)^{-1} \in F((x))$. So let $k = \min\{n : a_n \neq 0\}$ be the index of $\sum a_n x^n$, and define inductively

$$b_{-k} = a_k^{-1} \quad \text{and } b_{-k+n} = -a_k^{-1}\left(\sum_{\substack{i+j=n \\ k<j}} a_j b_j\right) \quad \text{for all } n \in \mathbf{N}.$$

Then $(\sum a_n x^n)(\sum b_n x^n) = \sum_{n\geq 0}\left(\sum_{i+j=n} a_i b_j\right)x^n = 1x^0 + 0x^1 + 0x^2 + \ldots = 1 \in F[[x]]$. Thus $(\sum a_n x^n)^{-1} = \sum b_n x^n$. We've demonstrated that $F((x))$ *contains* the field of fractions of $F[[x]]$. For the opposite containment, note that if K is a field containing $F[[x]]$, then $x, x^{-1} \in K$, and by linearity $F((x)) \subset K$. We conclude that the field of formal Laurent series $F((x))$ is the smallest field containing the ring of formal power series $F[[x]]$, so $F((x))$ is the field of fractions of $F[[x]]$.

ii. To show $\mathbf{Q}((x))$ properly contains $F :=$ the field of fractions of $\mathbf{Z}[[x]]$, consider $e^x \in \mathbf{Q}((x))$. Suppose $e^x \in F$ for contradiction. There then must be integer power series $a'(x), b'(x) \in \mathbf{Z}[[x]]$ to clear the denominators of e^x, i.e., such that $a'(x)e^x = b'(x)$. Choose $a(x) \in \mathbf{Z}[[x]]$ of minimal index $I(a) = \min\{n : a_n \neq 0\}$ such that there exists $b(x) \in \mathbf{Z}[[x]]$ with

$$a(x)e^x = b(x).$$

Explicitly, that's

$$\left(\sum_{n\geq I(a)} a_n x^n\right)\left(\sum_{n\geq 0}\frac{x^n}{n!}\right) = \left(\sum_{n\geq 0} b_n x^n\right).$$

Hence

$$\sum_{n\geq I(a)}\left(\sum_{i+j=n}\frac{a_i}{j!}\right) = \sum_{n\geq 0} b_n x^n.$$

So for all $n \geq I(a)$,

$$\left(\sum_{i+j=n}\frac{a_i}{j!}\right) - b_n = 0,$$

or, again for all $n \geq I(a)$, clearing denominators,

$$\frac{a_{I(a)}}{n - I(a)} + \underbrace{\ldots + a_n(n-(I(a)+1))! - b_n(n-I(a))!}_{\text{all integers}} = 0.$$

We observe that $a_{I(a)}$ is divisible by all natural numbers, which forces $a_{I(a)} = 0$, contradicting the choice of $a(x) = \sum_{n\geq I(a)} a_n x^n$ with minimal index. □

11.3. **[2, No. 7.6.1].** *Given.* An element $e \in R$ is called *idempotent* if $e^2 = e$. Assume e is idempotent in R and $er = re$ for all $r \in R$.

To prove.

i. Re and $R(1-e)$ are two-sided ideals of R.
ii. $Re \times R(1-e) \cong R$ as rings.
iii. e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.

Proof.

i. Let $re, se \in Re$ and $r(1-e), s(1-e) \in R(1-e)$ be arbitrary elements. Then

$$re - se = (r-s)e \in Re, \quad \text{and} \quad r(1-e) - s(1-e) = (r-s)(1-e) \in R(1-e).$$

For any $t \in R$, we have also

$$tre \in Re, \quad \text{and} \quad ret = rte \in Re$$

and

$$tr(1-e) \in R(1-e), \quad \text{and} \quad r(1-e)t = rt - ret = rt - rte = rt(1-e) \in R(1-e).$$

ii. Consider that $Re + R(1-e) \ni e + 1 - e = 1$. Moreover, $Re \cap R(1-e) \ni a$ implies $a = re$ and $a = s - se$, so $re = s - se$ hence $(r+s)e = s$ hence $(r+s)e^2 = se$ hence $re + se = se$ hence $se = 0$. So $a = 0$. We conclude the ideals Re and $R(1-e)$ are comaximal with trivial intersection. By [2, Sec. 5.4], we recognize $R \cong Re \times R(1-e)$ as additive groups. Now we take the associated isomorphism of groups $\varphi\colon R \to Re \times R(1-e)$ and check that φ is also ring homomorphism (an isomorphism actually, as the kernel is still trivial). We verify multiplicativity:

$$\varphi(re + s(1-e))\varphi(te + v(1-e)) = \varphi(rte, sv(1 - 2e + e^2)) = \varphi(rte + sv(1-e)).$$

iii. Consider the coordinate subrings Re and $R(1-e)$. If $re \in Re$, then $ere = re^2 = re = ree$, so e is the identity of Re. Likewise, if $r(1-e) \in R(1-e)$, then $(1-e)r(1-e) = r - re - er + ere = r(1-e)$. Similarly, $r(1-e)^2 = r(1-2e+e^2) = r(1-e)$. So $1-e$ is the identity for $R(1-e)$. □

11.4. **[2, No. 7.6.6].** *Given.* Let $f_1(x), f_2(x), \ldots, f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs ($\gcd(n_i, n_j) = 1$ for all $i \neq j$).

To prove.

i. There exists a polynomial $f(x)$ with integer coefficients and of degree d with $f(x) \equiv f_1(x) \pmod{n_1}$, $f(x) \equiv f_2(x) \pmod{n_2}$, $\ldots$, $f(x) \equiv f_k(x) \pmod{n_k}$, i.e., the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \pmod{n_i}$.
ii. If all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic.

Proof.

i. Because in $\mathbf{Z}$ the ideals $n_i\mathbf{Z}$ are pairwise comaximal, in $\mathbf{Z}[x]$ the ideals $n_i\mathbf{Z}[x]$ are also pairwise comaximal. (Observe for a ring R and ideals $\mathfrak{a}, \mathfrak{b} \subset R$, it's true that $(\mathfrak{a} + \mathfrak{b})[x] = \mathfrak{a}[x] + \mathfrak{b}[x]$, for $\sum(a_n + b_n)x^n = \sum a_n x^n + \sum b_n x^n$.) By the CRT,

$$\varphi\colon \mathbf{Z}[x] \to \prod_1^k \mathbf{Z}[x]/n_i\mathbf{Z}[x]$$

is surjective. In lecture, we proved $\mathbf{Z}[x]/n_i\mathbf{Z}[x] \cong (\mathbf{Z}/n_i\mathbf{Z})[x]$. That φ is surjective implies:

$$\text{there exists } f \in \mathbf{Z}[x] \text{ with } f(x) \equiv f_i(x) \pmod{n_i} \text{ for all } i = 1, \ldots, k.$$

ii. Suppose the f_i are each monic. Why can f be chosen monic? Well, if the f_i are monic, the leading coefficient $a_{\ell_i} \equiv 1 \pmod{n_i}$ of each f_i. By the CRT, the system of congruences $a_\ell \equiv a_{\ell_i} \pmod{n_i}$ has integral solutions uniquely determined modulo $n = \prod n_i$. One such solution is $a_\ell = 1 \equiv 1 \pmod{n_i}$ (for all i), which corresponds to $f(x)$ with a leading coefficient $a_\ell = 1$. (Note in this case the degree of f does not change, only the leading coefficient.) □

11.5. **[2, No. 8.1.3].** *Given.* Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R.

To prove. Every nonzero element of R of norm m is a unit. Therefore, a nonzero element of norm zero (if such and element exists) is a unit.

Proof. Consider nonzero $a \in R$ of minimum norm. Now R is a nonzero ideal in itself, so that $R = (d)$ where d is any nonzero element of minimum norm in R [2, Sec. 8.1]. But $(d) = R$ if and only if d is a unit. Since a is of minimum norm, $(a) = R$ and thus a is a unit. We deduce that for any nonzero $b \in R$ with $N(b) = 0$, it's clear that b would be of minimum norm among nonzero elements of R, whence b would be a unit. □

11.6. **[2, No. 8.1.7].** *To find.* Generators for the following ideals in $\mathbf{Z}[i]$

- $(85, 1 + 13i)$,
- $(47 - 13i, 53 + 56i)$.

Demonstration. (We implement the extended Euclidean algorithm for the Gaussian integers.)

We have $(85, 1 + 13i) = (7 + 6i)$, observing

```
85       = -6i * (1 + 13i) + (7 + 6i)
1 + 13i = (1 + i) * (7 + 6i)
```

as well, we have $(47 - 13i, 53 + 56i) = (4 - 5i)$,

```
53 + 56i = (1 + i) * (47 - 13i) + (-7 + 22i)
47 - 13i = (-1 - 2i) * (-7 + 22i) + (4 - 5i)
-7 + 22i = (-2 - 3i) * (4 - 5i)
```

and in the PID $\mathbf{Z}[i]$, a gcd of a finite set of elements generates the smallest ideal containing that set of elements. □

11.7. **[2, No. 8.2.6].** *Given.* Let R be an entire ring and suppose that every *prime* ideal in R is principal.

To prove. We'll prove that every ideal of R is principal in the following fashion:

a. Let $\mathscr{S}$ be the set of ideals of R that are not principal is nonempty. Assuming $\mathscr{S} \neq \varnothing$, $\mathscr{S}$ has a maximal element under inclusion (which, by hypothesis, is not prime).

b. Let $\mathfrak{m}$ be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in \mathfrak{m}$ but $a \notin \mathfrak{m}$ and $b \notin \mathfrak{m}$. Let $\mathfrak{a} = (\mathfrak{m}, a)$ be the ideal generated by $\mathfrak{m}$ and a, let $\mathfrak{b} = (\mathfrak{m}, b)$ be the ideal generated by $\mathfrak{m}$ and b, and define $\mathfrak{q} = \{r \in R : r\mathfrak{a} \subset \mathfrak{m}\}$. Then $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$ are principal ideals in R with $\mathfrak{m} \subsetneq \mathfrak{b} \subset \mathfrak{q}$ and $\mathfrak{a}\mathfrak{q} \subset \mathfrak{m}$.

c. If $x \in \mathfrak{m}$, then $x = s\alpha$ for some $s \in \mathfrak{q}$, forcing a contradiction: $\mathfrak{m} \subsetneq \mathfrak{b} \subset \mathfrak{q} \subset \mathfrak{m}$. Therefore $\mathscr{S}$ must have been empty, whence R is a PID.

Proof.

a. Let $\mathscr{S}$ be a poset of ideals ordered by inclusion, as above. Assume $\mathscr{S} \neq \varnothing$. Consider a chain of ideals $(\mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2, \ldots)$ in $\mathscr{S}$. Let $\bar{\mathfrak{a}} = \cup_{n \geq 0} \mathfrak{a}_i$. If $\bar{\mathfrak{a}}$ is not in $\mathscr{S}$, then $\bar{\mathfrak{a}} = (a)$ for some $a \in R$. But then $a \in \mathfrak{a}_n$ for some n, hence $\mathfrak{a}_n \subset \bar{\mathfrak{a}} \subset \mathfrak{a}_n$, forcing $\mathfrak{a}_n$ to be principal. So $\bar{\mathfrak{a}} \in \mathscr{S}$ is a bound for the chain of ideals $(\mathfrak{a}_0, \mathfrak{a}_1, \ldots)$. By Zorn's lemma, a partially ordered set where every chain is bounded above has a maximal element. So $\mathscr{S}$ has a maximal element, call it the ideal $\mathfrak{m}$.

b. Suppose $ab \in \mathfrak{m}$ with $a \notin \mathfrak{m}$ and $b \notin \mathfrak{m}$. Let $\mathfrak{q} = \{r \in R : r\mathfrak{a} \subset \mathfrak{m}\}$, where $\mathfrak{a} = (\mathfrak{m}, a)$ and $\mathfrak{b} = (\mathfrak{m}, b)$. Since $\mathfrak{a}$ and $\mathfrak{b}$ are not in $\mathscr{S}$, we have $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$ for some $\alpha, \beta \in R$.

- Is $\mathfrak{q}$ an ideal? Yes, for with $r, s \in \mathfrak{q}$, both $(r+s)\mathfrak{a} = r\mathfrak{a} + s\mathfrak{a} \subset \mathfrak{m}$ and so too $(rs)\mathfrak{a} = r(s\mathfrak{a}) \subset r\mathfrak{m} \subset \mathfrak{m}$.
- Does $\mathfrak{q}$ contain $\mathfrak{b}$? Yes. Multiplying generators, $\mathfrak{a}\mathfrak{b} = (\mathfrak{m}, a)(\mathfrak{m}, b) = (\mathfrak{m}^2, \mathfrak{m}b, \mathfrak{m}a, ab) \subset \mathfrak{m}$ as $ab \in \mathfrak{m}$. So if $r\beta \in \mathfrak{b}$, then $r\beta\mathfrak{a} \subset \mathfrak{m}$.
- We conclude $\mathfrak{m} \subsetneq \mathfrak{b} \subset \mathfrak{q}$ as $\mathfrak{m}$ is maximal among nonprincipal ideals, and is thus properly contained in $\mathfrak{b}$.

Commutativity and the definition of $\mathfrak{q}$ implies $\mathfrak{a}\mathfrak{q} = \mathfrak{q}\mathfrak{a} \subset \mathfrak{m}$.

c. Now to argue for contradiction. Say $x \in \mathfrak{m}$. Then $x = s\alpha$ for some $s \in R$. But $s\mathfrak{a} = s(\alpha) = (x)$, so $(x) \subset \mathfrak{m}$ implies $s\mathfrak{a} \subset \mathfrak{m}$, forcing $x \in \mathfrak{q}$. Thus $\mathfrak{m} \subsetneq \mathfrak{b} \subset \mathfrak{q} \subset \mathfrak{m}$, which is absurd. □

11.8. **[2, No. 8.2.7].** *Given.* An entire ring R in which every ideal generated by two elements is principal (i.e., for every $a, b \in R$, $(a, b) = (d)$ for some $d \in R$) is called a *Bézout Domain.*

To prove.

a. An entire ring R is a Bézout Domain if and only if every pair of elements a, b of R has a g.c.d. d in R that can be written as an R-linear combination of a and b. (That is, $d = ax + by$ for some $x, y \in R$.)

b. Every finitely generated ideal of a Bézout Domain is principal.

c. Let F be the fraction field of the Bézout Domain R. Every element of F can be written in the form a/b with $a, b \in R$ and a relatively prime to b.

Proof.

a. In one direction, say R is a Bézout domain. Then $(a, b) = (d)$ for any two elements $a, b \in R$. Then $d \in (a, b)$, and is of the form $d = ra + sb$ for some $r, s \in R$. Now $(d) \supset (a)$ and $(d) \supset (b)$. With any other divisor $(d') \supset (a)$ and $(d') \supset (b)$, we'd have $(d') \cap (a, b) = (d)$. So d is a gcd of a and b.

   Conversely suppose any two elements $a, b \in R$ have a gcd d that can be written as a R-linear combination $ra + sb = d$ for some $r, s \in R$. Then consider (a, b), the least ideal containing $\{a, b\}$. Let $\mathfrak{m}$ be another ideal containing $\{a, b\}$. Clearly $(a, b) \subset \mathfrak{m}$. Since $d = ra + sb$, we have also $(d) \subset \mathfrak{m}$. Moreover, $(d) \supset (a)$ and $(d) \supset (b)$, as d is a common divisor.[1] So (d) is the smallest ideal containing (a, b), hence $(d) = (a, b)$.

b. We proceed by induction on the size n of the finite generating set X_n of elements of R. Say X_2 is done for a base case (we're in a Bézout domain). Now suppose every ideal generated by X_{n-1} is principal. Consider (X_n). But this ideal is just (X_{n-1}, r_n) for $r_i \in X_n$. By the inductive hypothesis, $(X_{n-1}) = (d)$, so $(X_n) = (d, r_n)$. Being in a Bézout domain, $(d, r_n) = (\delta)$ for some $\delta \in R$, completing the induction.

c. We know an element of F is of the form rs^{-1} for $r \in R$ and $s \in R \setminus \{0\}$. Consider $d \in \mathrm{GCD}(r, s)$. We know both $(r, s) = (d)$ and there exist $x, y \in R$ such that $rx + sy = d$ (perhaps multiplying through by a unit). Since $r \in (d)$ and $s \in (d)$, we can write $r = ad$ and $s = bd$. So the R-linear combination becomes

$$d = adx + bdy, \quad \text{or} \quad 1 = ax + by,$$

   where $(a, b) = (1)$. Here, a and b are coprime and $\frac{r}{s} = \frac{ad}{bd} = \frac{a}{b}$. □

[1] TODO: revise.

11.9. **[2, No. 8.2.8].** *Given.* R is a PID and D is a multiplicatively closed subset of $R \setminus \{0\}$.

To prove. The ring of fractions $D^{-1}R$ is a PID.

Proof. If R is entire, then R has no zero divisors. Consider $\frac{r}{s}, \frac{t}{v} \in D^{-1}R$. If $\frac{rt}{sv} = 0$, then $rt = 0$. Either r or t is 0 in R, whence either $\frac{r}{s}$ or $\frac{s}{t}$ is 0 in $D^{-1}R$. To argue that $D^{-1}R$ is a PID, let $\mathfrak{q}$ be an ideal in $D^{-1}R$. Fix $d \in D$. Let $\mathfrak{p} \subset R$ be the ideal defined

$$p := \{r \in R : \frac{r}{d} \in \mathfrak{q}\}.$$

- Note $\mathfrak{p}$ contains 0.
- If $\mathfrak{p}$ contains r and t, then $\frac{r}{d} + \frac{t}{d} = \frac{r+t}{d} \in \mathfrak{q}$.
- If $\mathfrak{p}$ contains r, then $\frac{r}{d} \in \mathfrak{q}$. For any $t \in R$, we'd have $\frac{rt}{d} \in \mathfrak{q}$.

Because $\mathfrak{p} \subset R$ is a PID, there's $p \in R$ such that $(p) = \mathfrak{p}$. We'll now argue that $\mathfrak{q} \subset D^{-1}R$ is principal, namely that $\mathfrak{q} = (p/d)$. For one containment, let $s^{-1}q \in \mathfrak{q}$. Then $(d^{-1}s)s^{-1}q \in \mathfrak{q}$. So $\frac{q}{d} \in \mathfrak{q}$. Thus $q \in \mathfrak{p}$. We take the multiple $q = tp$ for some $t \in R$. Equating the two expressions of q,

$$s^{-1}q = s^{-1}tp = s^{-1}dd^{-1}tp = s^{-1}dt \cdot \frac{p}{d} \in \left(\frac{p}{d}\right).$$

For the other containment, take any $t \in R$, and observe by definition of $\mathfrak{q}$ we have $\frac{p}{d}t \in \mathfrak{q}$. Whence $\left(\frac{p}{d}\right) = \mathfrak{q}$. We conclude $D^{-1}R$ is a PID. □

11.10. **[2, No. 8.3.2].** *Given.* Let a and b be nonzero elements of the UFD R.

To prove. Then a and b have a least common multiple.

Demonstration. We describe a least common multiple of a and b in terms of the prime factorizations of a and b:

- Let $\{p_i\}_1^n$ be the set of distinct primes (irreducibles) in the unique factorization of the product ab.
- Choose exponents $\alpha_i, \beta_i \in \mathbf{Z}_{\geq 0}$ such that $a = \prod_1^n p_i^{\alpha_i}$ and $b = \prod_1^n p_i^{\beta_i}$.
  - These factorizations are unique up to associates, and we allow for zero exponents.
- Let $e = \prod_1^n p_i^{\max\{\alpha_i, \beta_i\}} \in R$.
- Verify that $e \in (a)$ and $e \in (b)$:
  - $e = \left(\prod_1^n p_i^{\max\{0, \alpha_i - \beta_i\}}\right) a$, similarly
  - $e = \left(\prod_1^n p_i^{\max\{0, \beta_i - \alpha_i\}}\right) b$.
- Suppose $e' = ra$ and $e' = sb$. Consider $ra = sb$.
  - Now r has a unique prime factorization
$$r = \left(\prod_1^n p_i^{\gamma_i}\right)\left(\prod_1^m t_j^{\rho_j}\right)$$
    with the p_i as before and the primes t_j distinct from the p_i.
  - Because $ra = sb$, for each $i = 1, \dots, n$ we must have $\gamma_i \geq \max\{\alpha_i, \beta_i\}$.
  - So then $e' = ra = \left(\prod_1^n p_i^{\alpha_i + \gamma_i}\right)\left(\prod_1^m t_j^{\rho_j}\right)$.
  - Because $\gamma_i + \alpha_i \geq \max\{\alpha_i, \beta_i\}$, we have $e' \in (e)$.

Now we've given an explicit construction of a least common multiple of a and b, namely $e \in R$. □

11.11. **[2, No. 8.3.6].** *Given.* We work in the Gaussian integers $\mathbf{Z}[i]$.

To demonstrate.

a. The quotient ring $\mathbf{Z}[i]/(1+i)$ is a field of order 2.
b. Let $q \in \mathbf{Z}$ be a prime with $q \equiv 3 \mod 4$. The quotient ring $\mathbf{Z}[i]/(q)$ is a field with q^2 elements.

c. Let $p \in \mathbf{Z}$ be a prime with $p \equiv 1 \mod 4$ and write $p = \pi\bar{\pi}$ as in Proposition 18.
   - The hypotheses for the Chinese Remainder Theorem (Theorem 17 in Section 7.6) are satisfied.
   - Moreover $\mathbf{Z}[i]/(p) \cong \mathbf{Z}[i]/(\pi) \times \mathbf{Z}[i]/(\bar{\pi})$ as rings.
   - The quotient ring $\mathbf{Z}[i]/(p)$ has order p^2.
   - Therefore, $\mathbf{Z}[i]/(\pi)$ and $\mathbf{Z}[i]/(\bar{\pi})$ are both fields of order p.

Demonstration.

a. When is $a + bi \in (1+i)$? Precisely when long division of $a+bi$ by $1+i$ in $\mathbf{Z}[i]$ has no remainder, that's exactly when
$$\frac{a+bi}{1+i} = \frac{(a-b)+(a+b)i}{2} \in \mathbf{Z}[i].$$
That is,
$$a-b \equiv 0 \pmod 2 \quad \text{and} \quad a+b \equiv 0 \pmod 2 \quad \text{if and only if} \quad a+bi \in (1+i).$$
It's true for all $a \in \mathbf{Z}$ that $2a \equiv 0 \pmod 2$, so always $(a+b)+(a-b) \equiv 0 \pmod 2$. This means either both the sum and the difference of a and b is *even*, or both the sum and the difference is *odd*. So $\mathbf{Z}[i]/(1+i)$ has only two equivalence classes, and is thus a ring isomorphic to the field $\mathbf{Z}/2\mathbf{Z}$.

b. Let $q \in \mathbf{Z}$ be prime and $\equiv 3 \pmod 4$. Then $a+bi \in (q)$ if and only if $\frac{a+bi}{q} \in \mathbf{Z}[i]$, if and only if (in $\mathbf{Z}$) $a \in (q)$ and $b \in (q)$. The q^2-1 nontrivial equivalence classes are index by distinct (modulo q) solutions $a, b \in \mathbf{Z}$ to $a \notin (q)$ or $b \notin (q)$. Because $\mathbf{Z}[i]$ is a PID and $(q) \subset \mathbf{Z}[i]$, a nonzero prime ideal, we know (q) is maximal. So the quotient $\mathbf{Z}[i]/(q)$ is a field, and counting by equivalence classes, $\mathbf{Z}[i]/(q)$ has q^2 elements.

c. Let $p \in \mathbf{Z}$ be prime, $\equiv 1 \pmod 4$ and consider $a, b \in \mathbf{Z}$ such that $p = [a+bi] * [a-bi]$.

   That $\mathbf{Z}[i](p)$ is a field of order p^2 follows from part b. Now consider the ideals $(a+bi)$ and $(a-bi$. Observe $p, 2a \in (a+bi)+(a-bi)$, where $p = (a+bi)(0+a-bi)$. Since $p > a^2$ and $p \equiv 1 \pmod 4$, $p \notin (2a)$. We see p and $2a$ are coprime (in the Gaussian integers). Thus $\mathbf{Z}[i] = (p, 2a) \subset (a+bi)+(a-bi)$ are comaximal ideals. Moreover $(p) = (a+bi) \cap (a-bi)$ (verify). The CRT implies $\mathbf{Z}[i]/(p) \cong \mathbf{Z}[i]/(a+bi) \times \mathbf{Z}[i]/(a-bi)$. Because neither coordinate subring is trivial, their orders must both be p. □

11.12. **Characterization of PIDs [2, No. 8.3.11].** *Given.* Let R be an entire ring.

To prove. R is a PID if and only if R is a UFD that is also a Bézout Domain.

Proof. ($\Rightarrow$) If R is a PID, then each element of R has a unique factorization into irreducibles [2, Sec. 8.3] and each ideal of R is principal. So R would be a Bézout UFD

($\Leftarrow$) Say R is a Bézout UFD. Let $\mathfrak{a}$ be an ideal in R. We aim to show $\mathfrak{a}$ is principal. Choose $a \in \mathfrak{a}$ such that $a = r_1 \cdots r - n$ has the minimum number of irreducible factors among elements of $\mathfrak{a}$. Suppose $b \in \mathfrak{a} \setminus (a)$ for contradiction. Say R is Bézout, so $\mathrm{GCD}(a,b) \ni d$, and $(d) = (a,b)$. Note b has $s_1 \cdots s_m$ irreducible factors with $m > n$. So $a \notin (b)$. As well, we assume $b \notin (a)$, so together this implies $d \neq b$. One should verify $d \neq b$ implies $(d) \supsetneq (a)$. We conclude d has fewer irreducible factors than a. But $d \in (a,b) \subset \mathfrak{a}$, which is absurd! We've discovered that $\mathfrak{a} \setminus (a)$ is empty, which forces $\mathfrak{a} \subset (a) \subset \mathfrak{a}$. Therefore $\mathfrak{a}$ is principal and R is a PID. □

References

[1] S. Lang, *Algebra.* 2002.

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