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

COLTON GRAINGER (MATH 6130 ALGEBRA)

11. Assignment due 2018-12-05

11.1. **[1, No. 7.5.4].** Any subfield of $\mathbf{R}$ must contain $\mathbf{Q}$.

11.2. **[1, No. 7.5.5].** If F is a field, the field of fractions of $F[[x]]$ (the ring of formal power series in the indeterminate x with coefficients in F) is the ring $F((x))$ of formal Laurent series. The field of fractions of the power series ring $\mathbf{Z}[[x]]$ is *properly* contained in the field of Laurent series $\mathbf{Q}((x))$ (hint: consider the series for e^x).

11.3. **[1, No. 7.6.1].** An element $e \in R$ is called *idempotent* if $e^2 = e$. Assume e is idempotent in R and $er = re$ for all $r \in R$. Re and $R(1-e)$ are two-sided ideals of R. e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.

11.4. **[1, No. 7.6.6].** Let $f_1(x), f_2(x), \dots, f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, \dots, n_k$ be integers which are relatively prime in pairs ($\gcd(n_i, n_j) = 1$ for all $i \neq j$). There exists a polynomial $f(x)$ with integer coefficients and of degree d with $f(x) \equiv f_1(x) \pmod{n_1}$, $f(x) \equiv f_2(x) \pmod{n_2}$, …, $f(x) \equiv f_k(x) \pmod{n_k}$, i.e., the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \pmod{n_i}$. If all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic. [Hint: apply the CRT in $\mathbf{Z}$ to each of the coefficients separately.]

11.5. **[1, No. 8.1.3].** Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. 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.

11.6. **[1, No. 8.1.7].** We find a generator for the ideal $(85, 1+13i)$ in $\mathbf{Z}[i]$, i.e., the greatest common divisor for 85 and $1+13i$. We find a generator for the ideal $(47-13i, 53+56i)$ as well. [Hint: use the Euclidean algorithm.]

11.7. **[1, No. 8.2.6].** Let R be an entire ring and suppose that every *prime* ideal in R is principal. (We'll prove that every ideal of R is principal.)

(a) Assume that the set of ideals of R that are not principal is nonempty. This set has a maximal element under inclusion (which, by hypothesis, is not prime). [Hint: use Zorn's Lemma.]

(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 $\mathfrak{a}\mathfrak{q} = (\alpha\beta) \subset \mathfrak{m}$.

(c) If $x \in \mathfrak{m}$, then $x = s\alpha$ for some $s \in \mathfrak{q}$. So $\mathfrak{m} = \mathfrak{m}_{\mathfrak{a}}\mathfrak{q}$ is principal, a contradiction. Therefore R is a PID.

Date: 2018-11-28.
Compiled: 2018-11-30.

11.8. **[1, No. 8.2.7].** 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 *Bezout Domain.*[1]

(a) An entire ring R is a Bezout 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 Bezout Domain is principal.[2]

(c) Let F be the fraction field of the Bezout Domain R. Every element of F can be written[3] in the form a/b with $a, b \in R$ and a relatively prime to b.

11.9. **[1, No. 8.2.8].** If R is a PID and D is a multiplicatively closed subset of R, then $D^{-1}R$ is also a PID.[4]

11.10. **[1, No. 8.3.2].** Let a and b be nonzero elements of the UFD R. Then a and b have a least common multiple.[5] We describe a least common multiple of a and b in terms of the prime factorizations of a and b.

11.11. **[1, No. 8.3.6].**

(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.

11.12. **Characterization of PIDs [1, No. 8.3.11].** R is a PID if and only if R is a UFD that is also a Bezout Domain.[6]

References

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

---

[1] See also [1, No. 8.3.11].

[2] See also [1, Sec. 9.2] and [1, Sec. 9.3] in which not every ideal is principal.

[3] See also [1, No. 8.2.1]

[4] See also [1, Sec. 7.5].

[5] See also [1, No. 8.1.11].

[6] One direction is given by Theorem 14. For the converse, let a be a nonzero element of the ideal $\mathfrak{a}$ with a minimum number of irreducible factors. Then prove $\mathfrak{a} = (a)$ by showing if there's an element $b \in \mathfrak{a}$ that's not in (a), then $(a, b) = (d)$ leads to a contradiction.