MAT 347
Factorization, GCDs, and ideals
January 8, 2019

Throughout this worksheet, R is always an integral domain; any unintroduced letter represents an element of R.

1 Primes and irreducibles

Definitions:

- Assume p is not a unit and not zero. p is called *irreducible* if whenever $p = ab$, either a is a unit or b is a unit.
- Assume p is not a unit and not zero. p is called *prime* if whenever $p|ab$, either $p|a$ or $p|b$.

1. Prove that every prime element is irreducible.

2 Factorization in terms of GCDs

Definitions:

- d is a *GCD* of a and b if it is a divisor of both a and b and, in addition, every other divisor of a and b divides d.
- Assume d is a GCD of a and b. We say that d *satisfies the Bézout identity* if there exist $x, y \in R$ such that $d = xa + yb$.
- R is a *GCD domain* if every pair of non-zero elements have a GCD.
- R is a *Bézout domain* if every pair of non-zero elements have a GCD which satisfies the Bézout identity.

2. Let S be the ring of polynomials with coefficients in $\mathbb{Q}$ which have no degree-one term, i.e. $S = \{a_0 + a_2X^2 + a_3X^3 + \cdots + a_nX^n : a_i \in \mathbb{Q}\}$. Note that this is a subring of $\mathbb{Q}[X]$.

    (a) Do the elements X^2 and X^3 have a GCD in S? If so, does it satisfy the Bézout identity?

(b) Do the elements X^5 and X^6 have a GCD in S? If so, does it satisfy the Bézout identity?

(Hint: consider degrees...)

3. Prove that every UFD is a GCD domain.

4. Prove that in a Bézout domain every irreducible element is a prime.

   Hint: Let p be irreducible. Assume $p|ab$. Let d be a GCD of p and a. Then...

3 Factorization in terms of ideals

5. For each of the following statement, write an equivalent statement in terms of ideals:

   (a) a is a unit.

   (b) a divides b.

   (c) a and b are associates.

   (d) p is irreducible.

   (e) p is prime.

   (f) c is a common divisor of a and b.

   (g) d is a GCD of a and b.

   (h) d is a GCD of a and b *and* there exist $x, y \in R$ such that $d = ax + by$.

   (i) R is a Bézout domain.

   (j) There exists a non-zero non-unit in R which cannot be written as a product of irreducible elements. (Update: show that this condition implies the existence of an infinite, strictly increasing chain of principal ideals. The converse is unfortunately not true...)

4 PIDs

Definition: A *principal ideal domain* (abbreviated PID) is an integral domain in which every ideal is principal.

6. Prove that every PID is a Bézout domain.

7. Prove that every PID is a UFD. (Hint: use your answers to questions 5i and 5j.)