MAT 347
Factorization, GCDs, and ideals
January 15, 2016

Throughout this worksheet, R is always an integral domain; any unintroduced letter represents an element on 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. Assume that factorization into irreducibles is unique in R. Prove that every irreducible element of R is prime.
3. Assume that every irreducible element of R is prime. Prove that factorization is unique in R.

2 Factorization in terms of GCDs

Definition:

- d is a *GCD* of a and b when 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* when there exist $x, y \in R$ such that $d = xa + yb$.
- R is a *GCD domain* when every pair of non-zero elements have a GCD.
- R is a *Bézout-domain* when every pair of non-zero elements have a GCD which satisfies the Bézout identity.

4. Let S be the ring of polynomials with coefficients in $\mathbb{Q}$ which have no degree-one term.
   (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?
5. Prove that every UFD is a GCD-domain.
6. 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

7. 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 divisor of a and a divisor or b.
   (g) d is a GCD of a and b.
   (h) There exists $x, y \in R$ such that $d = ax + by$.
   (i) R is a Bézout domain.
   (j) There exists an element in R which is not zero, not a unit, and cannot be written as product of irreducibles.

4 PIDs

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

8. Prove that every PID is a Bézout domain.
9. Prove that every PID is a UFD. (Hint: use your answers to questions **??** and **??**.)