Math 3032: Abstract Algebra

Practice final solutions

24 April 2023

Your name:

University academic honour statement:

Dalhousie University has adopted the following statement, based on "The Fundamental Values of Academic Integrity" developed by the International Center for Academic Integrity (ICAI):

> Academic integrity is a commitment to the values of learning in an academic environment. These values include honesty, trust, fairness, responsibility, and respect. All members of the Dalhousie community must acknowledge that academic integrity is fundamental to the value and credibility of academic work and inquiry. We must seek to uphold academic integrity through our actions and behaviours in all our learning environments, our research, and our service.

Please **sign here** to confirm that you will uphold these values, and that the work you submit on this exam will be your own.

Exam structure

There are six questions, each worth ten points.

Question 1.

Suppose that R is a unital commutative ring. State the definition of *zero-divisor* in R. Prove that $r \in R$ is *not* a zero-divisor if and only if the function $r \times (-) : R \to R$ is injective.

A *zero-divisor* is an element $r \in R$ such that there exists $s \neq 0$ with $rs = 0$. If such s exists, then $rs = r0$ and so $r \times (-)$ is not injective. Conversely, suppose that $r \times (-)$ is not injective, i.e. that $rs_1 = rs_2$ for some $s_1 \neq s_2$. Then $s = s_1 - s_2 \neq 0$, but, by the distributive law, $rs = 0$.

Question 2.

Suppose that $f : R \to S$ is a surjective ring homomorphism, and that R is unital. Show that S is also unital.

Let $1_R \in R$ denote the unit in R. We claim that $f(1_R) \in S$ is a unit. In other words, we claim that $f(1_R) \cdot s = s \cdot f(1_R) = s$ for all $s \in S$. But since f is surjective, for each $s \in S$ we can find a (nonunique!) $r \in R$ such that $s = f(r)$, and then, by using the multiplicativity of f, conclude that

$$f(1_R) \cdot s = f(1_R) \cdot f(r) = f(1_R \cdot r) = f(r) = s$$

and similarly on the other side.

Question 3.

When is an element of a ring called *irreducible*? When is it called *prime*? Give an example of an element of a ring which is irreducible but not prime. Give an example of an element of a ring which is prime but not irreducible.

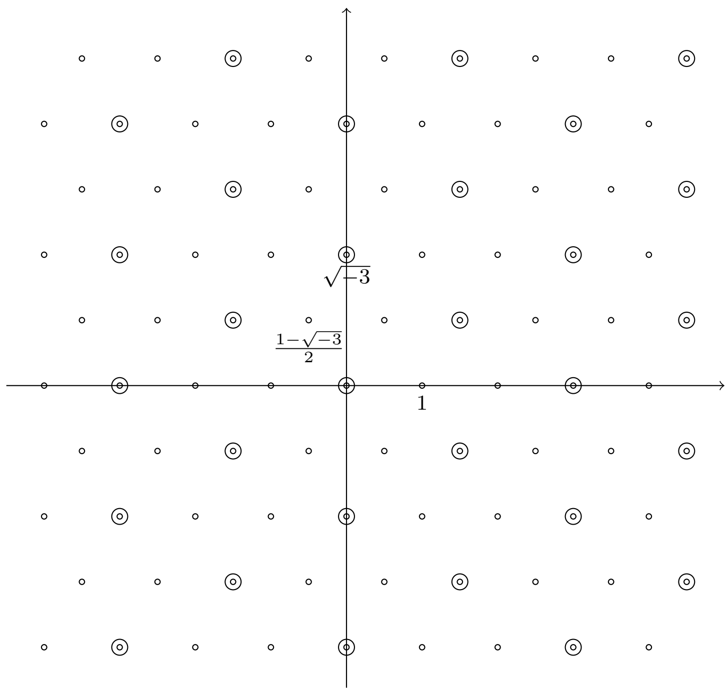
An element r is called *irreducible* if r is not invertible, and, whenever $ab = r$, one of a or b is invertible. An element r is called *prime* if, whenever ab is divisible by r, (at least) one of a or b is divisible by r.

An example of a prime but not irreducible element is $0 \in \mathbb{Z}$ (or any integral domain).

In $\mathbb{Z}$, and indeed in any UFD, every irreducible element is prime. But in $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible but not prime.

Question 4.

Draw a picture of the ideal $\langle\sqrt{-3}\rangle \subset \mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$.



Question 5.

Let R be a commutative ring. Recall that an element $r \in R$ is *nilpotent* ("zero-powered") if $r^n = 0$ for some $n \in \mathbb{N}$. Prove that the set of nilpotent elements is an ideal in R.

Unpacked, must prove the follow statements:

- If r, s are both nilpotent, then $r + s$ is nilpotent.
- If r is nilpotent and s is arbitrary, then rs is nilpotent.

For the second statement, suppose that $r^n = 0$. Then $(rs)^n = r^n s^n = 0s^n = 0$, so rs is nilpotent.

For the first statement, suppose that $r^n = 0$ and $s^m = 0$. Then

$$(r+s)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} r^i s^{m+n-i}.$$

Note that in each term in the sum, either $i \geq m$ or $m + n - i \geq n$. So either $r^i = 0$ or $s^{m+n-i} = 0$. So every term in the sum vanishes, and so the whole sum vanishes.

Question 6.

Run Buchberger's algorithm to find a Gröbner basis for the ideal $\langle x^2y + x, xy^2 - y\rangle \subset \mathbb{R}[x, y]$ **with respect to the ordering** $x \gg y$**.**

Since neither element head-divides the other, we first write down

$$s = S(x^2y + x, xy^2 - y) = y(x^2y + x) - x(xy^2 - y) = x^2y^2 + xy - x^2y^2 + xy = 2xy.$$

This is not head-divisible by either of $x^2y + x, xy^2 - y$, so we adjoin it, or rather half of it, to our basis. Now run long division by xy:

$$\begin{aligned} x^2y + x &\rightsquigarrow (x^2y + x) - x(xy) = x \\ xy^2 - y &\rightsquigarrow (xy^2 - y) - y(xy) = -y \end{aligned}$$

to produce the basis $\langle x, y, xy\rangle$. Note that xy is divisible by (both of) the other basis vectors, and so long division removes it from the basis. The final basis is $\langle x, y\rangle$, which is manifestly Gröbner.