MA434, Spring 2020 — Problem Day 2

The goal of this problem day is to review some Abstract Algebra and also to establish some basic theorems we will need. All of the problems are standard theorems you can find in your algebra textbook, but you should try to give proofs yourself. We may not have time to do them all in class, of course.

Throughout this problem set R will be a domain, i.e., a commutative ring (with 1) with $0 \neq 1$ and no zero-divisors.

1. Suppose R is a domain. Let K denote the set of all symbols $\frac{a}{b}$ with $a, b \in R$, $b \neq 0$, subject to the rule that

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc.$$

Define addition and multiplication in K and check that the resulting object is a field. K is called the *field of fractions* of R.

The examples we care the most about are these:

- If $R = \mathbb{Z}$ then $K = \mathbb{Q}$.
- If $R = k[x]$ is the ring of polynomials with coefficients in a field k, then $K = k(x)$ is the field of rational functions with coefficients in k.

2. Remember that an *ideal* in R is a subset $I \subset R$ which contains 0, is closed under addition, and "absorbs products," that is, if $r \in I$ and $x \in R$ then $rx \in I$. The easiest ideals are the *principal* ideals, which are just the set of all multiples of some fixed element $a \in R$:

$$I = Ra = (a) = \{ra \mid r \in R\}.$$

The next-easiest ideals are the *finitely-generated* ones, where

$$I = \{r_1a_1 + r_2a_2 + \cdots + r_ka_k \mid r_i \in R\}$$

for some finite set of $a_1, a_2, \ldots, a_n \in R$.

Conservatives believe in unchosen obligations, whereas classical liberals think that the only source of obligation is choice. – Roger Scruton

Let k be a field and let $R = k[x]$. Show that any ideal $I \subset R$ is principal. (If $I \neq \{0\}$, find an element $a \in I$ of minimal degree and prove that $I = Ra$.)

A domain in which every ideal is principal is called a *principal ideal domain*, or PID. The most important examples are $\mathbb{Z}$ and $k[x]$ when k is a field.

3. An ideal $I \subset R$ is called *maximal* if $I \neq R$ and there are no ideals "between" I and R: if J is an ideal and $I \subset J \subset R$ then either $I = J$ or $I = R$. Show that I is maximal if and only if R/I is a field.

4. An ideal $I \subset R$ is called *prime* if $ab \in I$ implies that either $a \in I$ or $b \in I$. Show that I is prime if and only if R/I is a domain.

5. Show that any maximal ideal is prime. Find an easy example of a prime ideal that is not maximal.

6. In a domain R, we have the subgroup $R^\times$ of all invertible elements of R; these elements are often called the *units* of R.

When $a, b \in R$ we say a divides b if there exists $x \in R$ such that $b = ax$. The units are exactly the divisors of 1. An element $a \in R$ is called *irreducible* if $a = bc$ implies that either b or c is a unit.

An element $b \in R$ is called *prime* if $b|xy$ implies that eigher $b|x$ or $b|y$. As you know, in $\mathbb{Z}$ these being irreducible is equivalent to being prime, but that is not true in a general domain. (Problem 11 gives an example.)

a. Show that if $a|b$ and $b|a$ then $a = ub$ for some unit $u \in R^\times$.

b. Show that if a is irreducible and u is a unit then ua is irreducible.

c. Show that if $a \in R$ is prime then it is irreducible.

d. Suppose you know that any irreducible element is prime. Prove that if $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ are all irreducble in R and we have

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

then $r = s$ and after reordering $p_i = u_1 q_i$ with $u_i \in R^\times$.

7. Let R be a domain. We say R is *Noetherian* if any increasing chain of ideals $I_1 \subset I_2 \subset I_3 \subset \ldots$ is actually finite, i.e., there must be a k such that $I_k = I_{k+1} = I_{k+2} = \ldots.$

Show that R is Noetherian if and only if every ideal $I \subset R$ is finitely generated.

8. Suppose R is Noetherian, $a \in R$, $a \neq 0$, $a \notin R^{\times}$. Show that there exist irreducibles $\pi_1, \pi_2, \ldots, \pi_k$ such that $a = \pi_1 \pi_2 \ldots \pi_k$. In other words, factorizations exist.

9. Suppose R is a PID.

a. Show that R is Noetherian, and conclude that any non-unit, non-zero element of R factors as a product of irreducibles.

b. Show that a is irreducible if and only if Ra is maximal.

c. Show that a is prime if and only if Ra is a prime ideal.

d. Conclude that any irreducible element of R is prime and therefore that factorizations in R are unique up to unit factors and order.

A domain where factorizations exist and are unique is called a *unique factorization domain* or UFD. So this problem can be summarized as PID $\Longrightarrow$ UFD.

10. Show that if R is a UFD then every irreducible element of R is prime.

11. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. R is known to be a Noetherian domain. Let $N : R \longrightarrow \mathbb{Z}$ be the function $N(a + b\sqrt{-5}) = a + 5b^2$. Since this is just the square of the complex absolute value, we know that $N\alpha\beta) = N(\alpha)N(\beta)$. (Of course, it's easy to check that by hand as well.)

a. Show that u is a unit in R if and only if $N(u) = 1$.

b. Show that no element of R has norm 3.

c. Show that no element of R has norm 7.

d. Show that 3, 7, $(1 + 2\sqrt{-5})$, and $(1 - 2\sqrt{-5})$ are all irreducible in R.

If you want to know what God thinks of money, just look at the people he gave it to. – Dorothy Parker

e. Check that $3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

f. What does that tell you?

12. (Gauss's Lemma) Suppose R is a UFD and K is its field of fractions. We want to compare factorizations in $R[x]$ and in $K[x]$. Let $f(x) \in R[x]$ and suppose we have $g(x), h(x) \in K[x]$ such that $f(x) = g(x)h(x)$. Show that there exists $a \in K$ such that $\tilde{g}(x) = ag(x) \in R[x]$, $\tilde{h}(x) = \frac{1}{a}h(x) \in R[x]$, and so $f(x) = \tilde{g}(x)\tilde{h}(x)$ is a factorization in $R[x]$.

(This one is hard. For any $f(x) \in R[x]$ we can factor out $c \in R$ so that $f(x) = cf_1(x)$ and the coefficients of $f_1(x)$ have no irreducible factors in common. We say $f_1(x)$ is *primitive*. The key is to show that the product of two primitive polynomials is primitive. It might be easier to do this for $\mathbb{Z}$ and $\mathbb{Q}$ first and then try to generalize.)

13. Suppose R is a UFD. Prove that $R[x]$ is a UFD.

14. Let k be a field. Show that the ring of polynomials $R = k[x_1, x_2, \ldots, x_n]$ is a UFD.

15. Suppose $f, g \in k[x, y]$ are polynomials in two variables with coefficients in a field k. Suppose $f(x, y)$ is irreducible and does not divide $g(x, y)$. Show that there are at most finitely many solutions to $f(x, y) = g(x, y) = 0$.

I've written several children's books . . . Not on purpose. – Steven Wright