MATH 7210 Homework 8

Andrea Bourque

November 2021

1 Problem 1

a) Let R be a PID. Show that R is unital.

Proof. Since R is trivially an ideal, we have that $R = (a)$ for some nonzero $a \in R$. Thus any element $r \in R$ can be expressed as $ab = r$ for some $b \in R$. In particular, there is some $c \in R$ such that $ac = a$. Then $rc = abc = acb = ab = r$ for all $r \in R$, so c is a multiplicative identity. $\square$

b) Exhibit a non-principal ideal in $2\mathbb{Z}$.

Proof. The whole ring itself is not a principal ideal. A principal ideal (a) in $2\mathbb{Z}$ has the form $\{..., -4a, -2a, 0, 2a, 4a, ...\}$. Since $a \in 2\mathbb{Z}$, all the elements of (a) will then be strictly contained in $4\mathbb{Z}$, so it cannot be equal to all of $2\mathbb{Z}$. $\square$

c) Show that the division algorithm fails in $2\mathbb{Z}$.

Proof. Consider $a = 6, b = 4$. Then there is no $q \in 2\mathbb{Z}$ such that $6 = 4q + r$ for $0 \leq r < 4$. This is because $q = 0$ gives $r = 6$ and $q = 2$ gives $r = -2$. Higher values of q will result in lower values of r, and lower values of q will result in higher values of r, so $r \geq 6$ or $r \leq -2$. Thus, the division algorithm fails. $\square$

2 Problem 2

Let F be a field and v a discrete valuation on F.

a) Show that $D = \{x \in F \mid v(x) \geq 0\}$ is a sub-integral domain of F containing 1 and that $M = \{x \in F \mid v(x) > 0\}$ is the unique maximal ideal of D.

Proof. Notice that $v(1) = v(1) + v(1)$, using the multiplicative property of v. Then $v(1) = 0$, so $1 \in D$. Since $v(0) = \infty$, $0 \in D$. For $x, y \in D$, $v(xy) = v(x) + v(y) \geq 0 + 0 = 0$, so $xy \in D$. $v(x+y) \geq \min(v(x), v(y)) \geq \min(0,0) = 0$, so $x + y \in D$. Thus D is a subring of F. Since F is an integral domain, D is as well.

That M is an ideal follows from the defining inequality and the definition of v. In particular, $v(x+y) \geq \min(v(x), v(y)) > \min(0,0) = 0$ for $x, y \in M$, and $v(xy) = v(x) + v(y) > v(x) \geq 0$ for $x \in D, y \in M$. Consider $D - M = \{x \in F \mid v(x) = 0\}$. If $v(x) = 0$, then $x \neq 0$, so $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) = v(x^{-1})$. Then $x^{-1} \in D$, so $D - M \subset D^{\times}$. Similarly, if $x \in D^{\times}$, then $0 = v(x) + v(x^{-1}) \geq v(x) \geq 0$ implies that $v(x) = 0$. Thus $D - M = D^{\times}$, implying that M is the unique maximal ideal of D. □

b) Suppose $a, b \in D$ and $b \neq 0$. Show that $b|a$ iff $v(a) \geq v(b)$. Conclude that v makes D into a Euclidean ring.

Proof. Suppose $a = bc$ for $c \in D$. Then $v(a) = v(bc) = v(b) + v(c) \geq v(b)$. If $v(a) \geq v(b)$, then $v(ab^{-1}) = v(a) - v(b) \geq 0$, so $ab^{-1} \in D$. If $v(a) < v(b)$, then $a = 0b + a$. Thus D has a division algorithm given by v. For $a, b \neq 0$, $v(ab) = v(a) + v(b) \geq v(a)$. Thus v is a Euclidean function on D. □

c) Let $\pi \in D$ satisfy $v(\pi) = 1$. Show that π is irreducible and that if $a \in F$ is nonzero, then a can be expressed uniquely as $u\pi^{v(a)}$, with $u \in D^{\times}$. Conclude that F is the quotient field of D.

Proof. Suppose $\pi = ab$ for $a, b \in D$. Then $1 = v(\pi) = v(a) + v(b)$. Since $v(a), v(b)$ are non-negative integers, the only possibility is that one of $v(a)$ or $v(b)$ is equal to 0, in which case one of a or b is a unit. Thus π is irreducible.

If $v(a) > 0$, then $v(\pi^{v(a)}) = v(\pi) + ... + v(\pi) = 1 + ... + 1 = v(a)$, where each sum has $v(a)$ terms. If $v(a) < 0$, we see that $0 = v(1) = v(\pi^{v(a)}\pi^{-v(a)}) = v(\pi^{v(a)}) - v(a)$, so $v(\pi^{v(a)}) = v(a)$. If $v(a) = 0$, then $1 = \pi^{v(a)}$, so $v(a) = 0 = v(\pi^{v(a)})$. Thus in any case, $v(a) = v(\pi^{v(a)})$. Then $v(a\pi^{-v(a)}) = 0$, implying $a\pi^{-v(a)} \in D^{\times}$. □

d) Show that the nonzero ideals of D are $(\pi^m) = \{x \in F \mid v(x) \geq m\}$ and that these are all distinct.

Proof. Let I be a nonzero ideal of D. Consider $v(I) = \{v(x) : x \in I\} \subset \mathbb{N} \cup \{0\}$. By the well-ordering principle of the natural numbers, $v(I)$ has a smallest element m. It follows that $I \subset \{x \in F \mid v(x) \geq m\}$. There is $x \in I$

such that $v(x) = m$. For some $u \in D^\times$, $x = u\pi^m$, so $\pi^m = u^{-1}x \in I$. Then $(\pi^m) \subset I$.

We now show that $(\pi^m) = \{x \in F \mid v(x) \geq m\}$, from which it will follow that $I = (\pi^m)$ by the inclusions $(\pi^m) \subset I \subset \{x \in F \mid v(x) \geq m\}$. We have $(\pi^m) \subset \{x \in F \mid v(x) \geq m\}$, so let $v(x) \geq m$. Since $v(\pi^m) = m \leq v(x)$, we have from part b that $\pi^m | x$, so $x = y\pi^m \in (\pi^m)$ for some $y \in D$. Thus $(\pi^m) = \{x \in F \mid v(x) \geq m\}$ as desired.

That these ideals are distinct follows from the inequality in $\{x \in F \mid v(x) \geq m\}$; if $\{x \in F \mid v(x) \geq m\} = \{x \in F \mid v(x) \geq n\}$ for $m \neq n$, say $m < n$ without loss of generality, then there is an element $x = \pi^m \in \{x \in F \mid v(x) \geq m\}$ with $v(x) = m < n$, so $v(x) \ngeq n$. $\square$

3 Problem 3

Show that each ring below is a DVR by defining an appropriate discrete valuation on its quotient field. Give explicit descriptions of the units and ideals.

a) $F[[X]]$ where F is a field.

Proof. From previous homework, the fraction field is $F((X))$. Define $v(a_nX^n + ...) = n$, the degree of the lowest non-zero monomial. Since $(a_nX^n+...)(b_mX^m+...) = a_nb_mX^{n+m} + ...$, we see $v(xy) = v(x) + v(y)$. Since $(a_nX^n + ...) + (b_mX^m + ...) = a_nX^n + ...$ for $n < m$, we see $v(x + y) \geq \min(v(x), v(y))$, where the inequality comes from the possibility of terms cancelling when $n = m$ and $a_n = -b_m$. Since the least degree term for elements of $F[[X]]$ has degree at least 0, we see that $F[[X]]$ is a DVR. $\square$

b) $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ where p is a fixed prime number.

Proof. Note that $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Q}$, so the fraction field is $\mathbb{Q}$. Let $v(n)$ be the highest power of p dividing an integer n. Then extend v to $\mathbb{Q}$ by $v(\frac{a}{b}) = v(a) - v(b)$. Then v is a valuation on $\mathbb{Q}$ since it is a valuation on $\mathbb{Z}$. For $\frac{a}{b} \in \mathbb{Z}_{(p)}$, since $v(b) = 0$, $v(\frac{a}{b}) = v(a) \geq 0$, so $\mathbb{Z}_{(p)}$ is a DVR. $\square$

4 Problem 4

Let p be an odd prime.

a) Show that exactly half of the integers $1, ..., p-1$ are quadratic residues mod p.

Proof. Consider the map $x \mapsto x^2$ on $(\mathbb{Z}/p\mathbb{Z})^*$. By definition, the image are the nonzero (mod p) quadratic residues. The kernel consists of x such that $x^2 \equiv 1$. Then $p|(x-1)(x+1)$, so $p|(x-1)$ or $p|(x+1)$. Thus the kernel has two elements, 1 and $p-1$. By an isomorphism theorem, the image of quadratic residues has size $(p-1)/2$. $\square$

b) Let m be a positive integer which is not a perfect square. Consider the subring $S_m = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ of $\mathbb{R}$. Show that $I_p = \{a + b\sqrt{m} \mid p|a, b\}$ is an ideal of S_m.

Proof. Let $pa + pb\sqrt{m}, pc + pd\sqrt{m} \in I_p$. Then $(pa + pb\sqrt{m}) + (pc + pd\sqrt{m}) = p(a + c) + p(b + d)\sqrt{m} \in I_p$. For any $c + d\sqrt{m} \in S_m$, $(pa + pb\sqrt{m})(c + d\sqrt{m}) = p(ac + bdm) + p(ad + bc)\sqrt{m} \in I_p$. Thus I_p is an ideal of S_m. $\square$

c) If m is a quadratic nonresidue mod p, show that I_p is a maximal ideal of S_m and that S_m/I_p is a field having p^2 elements.

Proof. Let J be an ideal strictly containing I_p, and let $x + y\sqrt{m} \in J - I_p$. Then $(x - y\sqrt{m})(x + y\sqrt{m}) = x^2 - my^2 \in J$. If $p \nmid (x^2 - my^2)$, then by the Euclidean algorithm, $p \in J$ implies $1 \in J$, so $J = S_m$. Now suppose $p|(x^2 - my^2)$. Since $x + y\sqrt{m} \notin I_p$, $p \nmid x$ or $p \nmid y$. If $p \nmid y$, then y has an inverse z mod p. Then $x^2 \equiv my^2$ implies $(xz)^2 \equiv m$, which is a contradiction. Thus $p \nmid x$ and $p|y$. Since $p|y$, $y\sqrt{m} \in J$, so $x \in J$ also. Since $p \nmid x$ and $p \in J$, $\gcd(x, p) = 1$ implies $1 \in J$, so $J = S_m$. $\square$

5 Problem 7.6.3

Let R, S be unital rings. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.

Proof. Let $\pi_1 : R \times S \to R$ be the projection $\pi_1(r, s) = r$, and let $\pi_2 : R \times S \to S$ be the projection $\pi_2(r, s) = s$. π_1, π_2 are surjective ring homomorphisms. Let K be an ideal of $R \times S$, and let $I = \pi_1(K), J = \pi_2(K)$. Since the image of an ideal in a surjective ring homomorphism is an ideal, I is an ideal of R and J is an ideal of S.

If $(a, b) \in K$, then $a = \pi_1(a, b) \in I$ and $b = \pi_2(a, b) \in J$, so $(a, b) \in I \times J$. Thus $K \subset I \times J$. If $(a, b) \in I \times J$, then $(a, s) \in K$ for some $s \in S$ and $(r, b) \in K$ for some $r \in R$. Then $(1, 0)(a, s) = (a, 0) \in K$ and $(0, 1)(r, b) = (0, b) \in K$, so $(a, 0) + (0, b) = (a, b) \in K$. Thus $K = I \times J$. $\square$