

Tutorial 5

1. Let R be a principal ideal domain and $p \in R$ an irreducible element. Prove that R/pR is a field as follows. Show that if $a \in R$ is such that $p \nmid a$ then p and a have greatest common divisor 1. So there exist $r, s \in R$ with $ra + sp = 1$. Deduce that element $a + pR$ of the quotient ring R/pR has an inverse (namely, $r + pR$). Deduce that every non-zero element of R/pR has an inverse.

Solution.

An element $d \in R$ is a greatest common divisor of a and p if the following properties hold:

- (A1) $d|a$ and $d|p$;
 (A2) if $e|a$ and $e|p$ then $e|d$.

As proved in lectures, because R is P.I.D., such an element exists and for any such d there exist $m, n \in R$ with $ma + np = d$. (We also showed that any d with the property $aR + pR = dR$ is a greatest common divisor of a and p .)

We show $d = 1$ has properties A1 and A2. Then we can deduce it is a greatest common divisor of a and p and hence there $r, s \in R$ such that $ra + sp = 1$.

Trivially $1|p$ and $1|a$ property A1 is true for $d = 1$. Now suppose $e|p$ and $e|p$. To show A2. holds for $d = 1$ we must show $e|1$, i.e. e is a unit. From $e|p$ and p irreducible we conclude e is unit or an associate of p . In the case e is an associate of p we have both $e|p$ and $p|e$. But if e is an associate of p , $p|e$ which together with $e|a$ would give $p|a$, contradicting $p \nmid a$. So e must be a unit as required for A2.

To show that R/pR is a field we must show that it is a commutative ring with an identity element which is nonzero, such that every nonzero element has a multiplicative inverse.

The ring R/pR is commutative (since R is) and has an identity element (since R has). Indeed, the element $1 + pR$ is the identity. We do not have $1 + pR = 0 + pR$ because this is only the case if $p|1$, and so p is a unit. But p is irreducible and part of the definition of p irreducible is p not a unit. It remains to show the non-zero elements in R/pR are invertible.

The non-zero elements of the quotient ring are the $a + pR$ with $p \nmid a$. For such a we have an equation $ra + sp = 1$ in R which gives an equation $rs + pR = 1 + pR$ in

R/pR . Hence

$$(r + pR)(a + pR) = ra + pR = 1 + pR$$

In view of commutativity, this shows that $r + pR$ is an inverse of $a + pR$. (And remember that inverses are unique; so we can say that $r + pR$ is *the* inverse of $a + pR$.)

2. An ideal I in a ring R is said to be *prime* if $I \neq R$ and the following condition is satisfied:

$$\text{for all } a, b \in R, \text{ if } ab \in I \text{ then } a \in I \text{ or } b \in I.$$

Let R be a commutative ring with 1 and I an ideal in R . Prove that I is prime if and only if R/I is an integral domain.

Solution.

Assume that I is a prime ideal in R . Let $\alpha, \beta \in R/I$ such that $\alpha\beta = 0$. Elements of R/I are cosets of I in R ; the zero element of R/I is the ideal I itself ($= 0 + I$), while $\alpha = a + I$ and $\beta = b + I$ for some (arbitrarily chosen) representative elements $a \in \alpha$ and $b \in \beta$. By the definition of multiplication in R/I we deduce that $ab + I = (a + I)(b + I) = \alpha\beta = 0 + I$, and hence $ab \in I$. Since I is prime either $a \in I$ or $b \in I$, and thus either $a + I = I$ or $b + I = I$. That is, either α or β must be the zero element of R/I . So we have shown that R/I has no zero divisors. Since R is commutative and has a 1 the same is true for R/I . Hence R/I is an integral domain.†

Conversely, assume that R/I is an integral domain. Suppose $a, b \in R$ satisfy $ab \in I$. Then $ab + I = I$, which is the zero element of the quotient ring R/I . By the definition of multiplication in R/I it follows that $(a + I)(b + I) = ab + I = I$, and since R/I has no zero divisors we can conclude that either $a + I = I$ or $b + I = I$. That is, either $a \in I$ or $b \in I$. So we have shown that for all $a, b \in R$, if $ab \in I$ then $a \in I$ or $b \in I$. That is, the ideal I is prime.‡

3. (Third Isomorphism Theorem) Let I and J be ideals in the ring R with $I \subseteq J$. Show that $a + I \mapsto a + J$ for all $a \in R$ defines a surjective homomorphism $R/I \rightarrow R/J$. Use the First Isomorphism Theorem to deduce that J/I is an ideal in R/I and $(R/I)/(J/I) \cong R/J$.

Now conversely suppose that K is an ideal of R/I . Show that the kernel of the composite of the canonical map from R to R/I and the canonical map from R/I to $(R/I)/K$, $J = \{x \in R : x + I \in K\}$ is an ideal of R containing I such that $K = J/I$.

† One of the integral domain axioms, which is sometimes overlooked, is that it is non-zero ring. The assumption $I \neq R$ ensures R/I is not the zero ring.

‡ And we should have proved that $I \neq R$, since this is part of the definition of prime. The fact that R/I is an integral domain implies that $1 + I \neq 0 + I$; hence $1 \notin I$, and hence $I \neq R$.

Solution.

Let $a, b \in R$ with $a+I = b+I$. Since cosets are defined as equivalence classes for the relation of congruence modulo the ideal (see lectures) we conclude that $a \equiv b \pmod{I}$; that is, $a - b \in I$. Since $I \subseteq J$ it follows that $a - b \in J$, and hence $a + J = b + J$. So there is a well defined function $\phi: R/I \rightarrow R/J$ such that $\phi(a + I) = a + J$ for all $a \in R$.

This function ϕ is trivially a homomorphism, since by the definition of addition and multiplication in quotient rings we have

$$\begin{aligned}\phi((a + I) + (b + I)) &= \phi((a + b) + I) = (a + b) + J \\ &= (a + J) + (b + J) = \phi(a + I) + \phi(b + I)\end{aligned}$$

$$\phi((a + I)(b + I)) = \phi(ab + I) = ab + J = (a + J)(b + J) = \phi(a + I)\phi(b + I)$$

for all $a, b \in R$, and so $\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$ and $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ for all $\alpha, \beta \in R/I$ (since every element of R/I has the form $a + I$ for some $a \in R$). It is also (trivially) surjective since every element of R/J has the form $a + J = \phi(a + I)$ for some $a \in R$.

Since ϕ is surjective its image is R/J . The kernel of ϕ is

$$\begin{aligned}\{\alpha \in R/I \mid \phi(\alpha) = 0 + J\} &= \{a + I \mid a \in R \text{ and } a + J = J\} \\ &= \{a + I \mid a \in J\},\end{aligned}$$

which by definition is J/I . (Note that the fact that I is an ideal of R which is contained in the subring J of R implies that I is also an ideal in J , as follows immediately from the definition of “ideal”.) The First Isomorphism Theorem gives $(R/I)/\ker \phi \cong \text{im } \phi$; that is $(R/I)/(J/I) \cong R/J$.

Recall both canonical maps are ring homomorphisms and hence so is their composite. If $x \in R$ then by the first canonical map $x \mapsto x + I$ and the second $x + I \mapsto (x + I) + K$. So x is in the kernel of the composite if and only if $(x + I) \in K$. So the given set J is the kernel of the composite and so is an ideal. If $x \in I$ it maps to $x + I = I \in R/I$ under the first canonical map and then to $O \in (R/I)/K$ under the second. Hence $I \subseteq J$.

4. An ideal I in a ring R is said to be *maximal* if $I \neq R$ and the only ideals J in R such that $I \subseteq J$ are I and R .

Suppose that R is a commutative ring with 1 and that I is a maximal ideal in R . Show that if $a, b \in R$ are arbitrary elements such that $a \notin I$ then there exists $x \in R$ such that $b + I = ax + I$. (Hint: consider the ideal $I + aR$.) Deduce that R/I is a field.

Solution.

Let $a, b \in R$ with $a \notin I$. Since R is a commutative ring, aR is an ideal in R . Thus $I + aR \stackrel{\text{def}}{=} \{x + y \mid x \in I, y \in aR\}$ is an ideal in R , by Question 2 of Tutorial 2. If

x is any element of I then $x = x + 0 \in I + aR$ (since $0 = a0 \in aR$); so $I \subseteq I + aR$. Furthermore, since $0 \in I$ and $a1 \in aR$ it follows that $a = 0 + a1 \in I + aR$, and so $I + aR \neq I$ (since $a \notin I$). By maximality of I it follows that $I + aR = R$. Hence $b \in I + aR$, and so $b = t + ax$ for some $t \in I$ and $x \in R$. This shows that $b - ax \in I$; in other words, b is congruent to ax modulo I . This, in turn, means that $b + I = ax + I$.

Since R is a commutative ring with 1, so is R/I (see Tutorial 4, Question 2). Note that the 1 element of R/I is nonzero—that is, $1 + I \neq 0 + I$ —since $1 \notin I$ (since $I \neq R$). Now suppose that α is an arbitrary nonzero element of R/I . Then $\alpha = a + I$ for some $a \in R$ such that $a \notin I$, and by the first part of the question, applied with $b = 1$, we deduce that there exists an $x \in R$ such that $1 + I = ax + I$. The element $\beta = x + I \in R/I$ is an inverse of α , since $1 + I$ is the identity of R/I , and

$$\beta\alpha = (x + I)(a + I) = xa + I = ax + I = 1 + I = (a + I)(x + I) = \alpha\beta$$

(where we have used the fact that R is commutative). But α was an arbitrary nonzero element of R/I , and so we have shown that all nonzero elements of R/I have inverses. So R/I is a field.

5. Let R be a principal ideal domain. Show that a non-zero $p \in R$ is irreducible if and only if pR is a maximal ideal.

Solution.

Suppose $p \neq 0$ is not irreducible. Then either p is a unit and $pR = R$ is not maximal or there is an $a \in R$ such that $a|p$ and a is neither a unit nor associate of p . In terms of ideals this says $pR \subseteq aR$, but $pR \neq R$ and $aR \neq pR$, i.e. $pR \subsetneq aR \subsetneq R$. Hence pR is not a maximal ideal in the latter case. So if pR is a maximal ideal, p is irreducible.

Now suppose p is irreducible. So p is not a unit. Hence $pR \neq R$. Suppose I is an ideal and $pR \subseteq I$. We show either $I = R$ or $I = pR$ and hence pR is maximal. Because R is a P.I.D. $I = aR$ for some R and $pR \subseteq aR$. Hence $a|p$. So p irreducible implies either a is a unit or a is an associate of p , which in terms of ideals say either $aR = R$ or $aR = pR$.

6. How many distinct functions are there from the two-element field \mathbb{F}_2 to itself? How many of these are polynomial functions? And how many elements are there in $\mathbb{F}_2[x]$, the set of all polynomials over \mathbb{F}_2 in the indeterminate x ?

Solution.

Let $f: \mathbb{F}_2 \rightarrow \mathbb{F}_2$ be a function. There are two possibilities for each of $f(1)$ and $f(0)$; so four ($= 2 \times 2$) possibilities altogether for f . All four functions are polynomial functions, corresponding to the polynomials $0, 1, x$ and $x + 1$ in $\mathbb{F}_2[x]$. And $\mathbb{F}_2[x]$ has infinitely many elements: indeed, for each nonnegative integer n there are 2^n elements of degree n in $\mathbb{F}_2[x]$. (A polynomial has degree n if it has the form $a_0 + a_1x + \cdots + a_nx^n$

with $a_n \neq 0$. For polynomials over \mathbb{F}_2 the condition $a_n \neq 0$ becomes $a_n = 1$; there are 2 choices for each of the other n coefficients.)

Of course it follows from the above that there are distinct polynomials in $\mathbb{F}_2[x]$ giving rise to the same function. For example, observe that for every integer $n \geq 1$ the polynomial x^n yields the function $0 \mapsto 0$ and $1 \mapsto 1$.