

PRACTICE QUALIFYING EXAM

RING THEORY

R1. Let R be a commutative integral domain in which each prime ideal is principal. Prove or disprove that R is a P.I.D.

Proof. Suppose R is not a P.I.D. Let \mathcal{S} be the set of non-principal ideals of R , which is nonempty. It's easy to show that for any strictly ascending chains $I_1 \subsetneq I_2 \subsetneq \dots$ in \mathcal{S} , $I = \cup_{i=1}^{\infty} I_i$ is not principal (otherwise the generator of I must be in some I_n , this makes all $I_m = I$ principal for $m \geq n$). Hence we can apply Zorn's Lemma to \mathcal{S} to find a maximal element $I \in \mathcal{S}$.

If I is not prime, we can find $a, b \in R \setminus I$ with $ab \in I$. So $I \subsetneq I_a = I + aR$. Let $J = (I : I_a) := \{r \in R : rs \in I \text{ for all } s \in I_a\}$, then $b \in J \setminus I$, hence $I \subsetneq J$. By maximality of I in \mathcal{S} , we get $I_a = (\alpha)$ and $J = (\beta)$ for $\alpha, \beta \in R$.

$I_a J = (\alpha\beta) \subset I$ by definition of J . We will show $I \subset I_a J$. Take any $x \in I$, since $I \subset I_a = (\alpha)$, we can write $x = c\alpha$ for $c \in R$. Clearly $cI \subset I$ and $c\alpha = x \in I$, hence $cI_a \in I$ and $c \in J$. Then we can write $c = d\beta$ for $d \in R$. Then $x = d\alpha\beta \in I_a J$.

Thus we have shown that $I = I_a J = (\alpha\beta)$ is principal, which yields a contradiction unless I is a prime, but then I has to be principal by the assumption, this gives another contradiction. So R must be P.I.D..

A similar argument actually shows the following fact due to I.S. Cohen: If every prime ideal of a commutative ring R is finitely generated, then every ideal in R is finitely generated. □

R2. Let R be commutative ring, I be a prime ideal of $R[X]$ such that $R/(I \cap R)$ is a U.F.D. Prove or disprove that I is generated in $R[X]$ by $I \cap R$ and a single element of $R[X]$.

Proof. The statement is true. Look at classical residue epimorphism $\phi : R[X] \twoheadrightarrow R[X]/(I \cap R) \simeq (R/(I \cap R))[X]$. Let $S = R/(I \cap R)$ and $J = I/I \cap R$. Then S is a UFD by assumption, and J is a prime ideal in $S[X]$ ($S[X]/J \simeq R[X]/I$ is an integral domain) such that $J \cap S = \phi(I \cap R) = \{0\}$. If we know $J = (\bar{f})$ is generated by one element $\bar{f} \in S[X]$, then I is generated by $I \cap R$ and a single element $f \in R[X]$, where f is any element in $\phi^{-1}(\bar{f})$.

Hence we are reduced to showing that if S is a UFD and J is a prime ideal of $S[X]$ such that $J \cap S = \{0\}$, then J is a principal ideal. We need the following lemma about UFD (a form of Gauss's Lemma): Let S be a UFD, and $f, g \in S[X]$. Let $c(f)$ denote the G.C.D of the coefficients of f (called the content of f), then $c(fg) = c(f)c(g)$.

Now let us take a polynomial $f(X) \in J$ of minimal degree n . We get $f = c(f) \cdot g$ with a polynomial $g(X) \in S[X]$ of degree n and $c(g) = 1$. Since J is prime, if $g \notin J$, we must have $c(f) \in J \cap R = \{0\}$, impossible. Hence we obtain a polynomial $g(X) \in J$ with minimal degree n and content $c(g) = 1$, we claim that $J = (g)$.

Take any $h \in J$, do the long division algorithm in $K[X]$ where K is the quotient field of S , we get $h = ag + b$ with $a, b \in K[X]$ such that $b = 0$ or b has degree less than n . Clear the denominator we get $sh = a'g + b'$ with $s \in S$ and $a' = sa \in S[X], b' = sb \in S[X]$. Now $b' = sh - a'g \in J$ is either 0 or has degree $< n$. By the minimality of the degree of g in J , we must have $b' = 0$, hence $sh = a'g$, but $sc(h) = c(a')c(g) = c(a')$, we must have $a'/s \in S[X]$, so $h \in (g)$. \square

R3. Let R be a commutative integral domain such that the greatest common divisors of any two non-zero elements (e.g., d divides a and b and is divisible by any element e with the same property) always exist in R . Show that any irreducible element in R is prime.

Proof. It's easy to show that any two G.C.D of a and b are associated to each other. Abusing the language, we will use (a, b) to denote a G.C.D of a and b , and use " $=$ " to denote that two elements are associated. We claim the following property about G.C.D: if $(x, z) = 1$ and $(y, z) = 1$, then $(xy, z) = 1$.

If this is true, we can then show that any irreducible element $r \in R$ is prime. If $a, b \in R$ such that $ab \in (r)$, then $(ab, r) = r$. If $a \notin (r)$, then (a, r) divides r , but is not associated to r . As r is irreducible, we must have $(a, r) = 1$. If also $b \notin (r)$, then $(b, r) = 1$ by the same argument, hence $(ab, r) = 1$ by our claim, which is impossible. So either a or b must be in (r) , and r is prime.

Now it suffices to prove the claim. First, let's note that $(xz, yz) = (x, y)z$. This is because (x, y) divides both x and y , $(x, y)z$ certainly divides xz and yz , hence (xz, yz) . But z is a common divisor of xz, yz , hence divides (xz, yz) , write $(xz, yz) = ez$, we have $ez|xz$ implies $e|x$ in the domain R , similarly $e|y$. So $e|(x, y)$, then $(xz, yz) = ez$ divides $(x, y)z$. Hence $(xz, yz) = (x, y)z$. Now suppose $(x, z) = 1 = (y, z)$, if $(xy, z) = d$. Write $xy = ed, z = fd$, we have $y = (x, z)y = (xy, zy) = (ed, zfd) = (e, zf)d$, hence $d|y$. Then $d|(y, z) = 1$. Hence $(xy, z) = 1$, we are done. \square

R4. R is a ring (not necessarily commutative) with identity. Consider the following two conditions:

- (I) For any $a, b \in R, ab = 0 \implies ba = 0$;
- (II) For any $a, b \in R, ab = 1 \implies ba = 1$.

Show that I implies II, and show by example that II does not imply I.

Proof. We want to show that I implies II. Let $ab = 1$ for some $a, b \in R$. Then $aba = a$, i.e., $a(ba - 1) = 0$ implies $(ba - 1)a = 0$, i.e., $ba^2 = a$, multiply both side by b from the left hand side, we get $ba = baab = ab = 1$. Hence I implies II. In the matrix ring $M_2(\mathbb{Z})$, we know II always holds as it is a group. But $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq 0 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ \square

R5. R is a commutative integral domain such that any strictly ascending chain of ideals is finite, i.e., $I_0 \subsetneq I_1 \subsetneq \dots \subsetneq I_n \subsetneq \dots$ must stop after finitely many ideals. Prove that any non-zero and non-unit element in R is a product of irreducible elements.

Proof. Assume there is a non-zero non-unit $a \in R$ that is not a product of irreducible elements. Then a can't be irreducible, hence $a = a_1b_1$ for some non-units

a_1 and b_1 . Note that $(a) \subsetneq (a_1)$, otherwise b_1 would be a unit. At least one of a_1 and b_1 is not a product of irreducible elements by the assumption on a , we can assume that is a_1 , and write $a_1 = a_2 b_2$. Continue this way, we will get a strictly ascending chain of ideals:

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

which contradicts the ascending chain condition on R . Hence we can always write a non-zero and non-unit element in R as a product of irreducible elements. \square

R6 (Jan 96). Let R be a UFD with field of fractions F . Let $f, g \in R[X]$ be polynomials with no common roots in any field extension of F .

(a) Show that there exist $h, k \in R[X]$ and $0 \neq d \in R$ such that $hf + kg = d$. Is d the greatest common divisor of f and g ? Justify your answer.

(b) When $R = \mathbb{Z}$, show that the ideal I of $\mathbb{Z}[X]$ generated by $f = x^2 + 4x + 5$ and $g = x^2 + x + 1$ is maximal and determine the field $\mathbb{Z}[X]/I$.

Proof. (a) Let K be the quotient field of R . Since $K[X]$ is Euclidean, f, g has a g.c.d d' in $K[X]$. If $\deg(d') > 0$, then f, g share at least one common root, hence $\deg(d') = 0$ and $d' \in K$. d' being the g.c.d of f, g indicates that $af + bg = d'$ for $a, b \in K[X]$, clear the denominator we get $hf + kg = d$ for some $d \in R$ and $h, k \in R[X]$. Note that we don't really need any condition on R other than that R is an integral domain.

Unfortunately, d may not be the G.C.D of f, g . Take for example, $f = 2x + 9$ and $g = 4x + 5$ in $\mathbb{Z}[X]$, we can see $2f - g = 13$, but clearly 13 does not divide either f or g .

(b) It is not too hard to show that $13 \in I$, $\mathbb{Z}[X]/(13) \simeq \mathbb{F}_{13}[X]$, hence by isomorphism theorems $\mathbb{Z}[X]/I \simeq \mathbb{F}_{13}[X]/\bar{I}$ where $\bar{I} = I/(13)$. That shows we are reduced to the case of computing the ideal generated by f, g in $\mathbb{F}_{13}[X]$. But f, g share a common factor $x - 3$ (common root 3 over \mathbb{F}_{13}), hence $\bar{I} = (x - 3)\mathbb{F}_{13}[X]$. Then $\mathbb{Z}[X]/I \simeq \mathbb{F}_{13}[X]/(x - 3) \simeq \mathbb{F}_{13}$, and I must be a maximal ideal. \square

R7 (Jan 97). (a) Factor 2 into primes in $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$ and justify your answers.

(b) Show that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-n}]$ for any $n > 2$.

(c) For which $n > 0$ is $\mathbb{Z}[\sqrt{-n}]$ a UFD?

Proof. For any subring R of \mathbb{C} that is fixed by conjugation, define normal $N : R \rightarrow \mathbb{R}$ by $N(r) = ||r||^2$ for $r \in R$. The image $N(R)$ is a multiplicative subset of $R \cap (\mathbb{R}^+ \setminus \{0\})$. This norm has the following properties (try to prove them):

- N is multiplicative, $N(r) = 0$ iff $r = 0$;
- $N(r)$ is a "unit" in $N(R)$ iff r is a unit in R ;
- If $N(r)$ is "irreducible" in $N(R)$, then r is irreducible in R .

In particular, for $R = \mathbb{Z}[\sqrt{-n}]$, $N(R) = \mathbb{N}$, the quoted words unit and irreducible resume the normal meaning of their usages. We can hence use the norm to try to identify irreducible elements and units in the ring.

(a) $N(2) = 4 = 2 \times 2$.

In $\mathbb{Z}[i]$, if $2 = pq$ for non-units p and q , we must have $N(p) = N(q) = 2$, hence $2 = (1+i)(1-i)$ in $\mathbb{Z}[\sqrt{-1}]$. It is easy to check that $1 \pm i$ divides $a + bi$ in $\mathbb{Z}[i]$ iff a, b has the same parity, or equivalently, iff $a + b$ is even. So if $(a + bi)(c + di)$ is in, say,

$(1+i)R$, then $ac-bd+ad+bc$ must be even, hence so is $ac+bd+ad+bc = (a+b)(c+d)$. So either $a+b$ is even or $c+d$ is even, showing that at least one of $a+bi$ and $c+di$ must be in $(1+i)R$. So both $1 \pm i$ are primes in $\mathbb{Z}[i]$.

In $\mathbb{Z}[\sqrt{-2}]$, clearly $2 = -\sqrt{-2}^2$ in $\mathbb{Z}[\sqrt{-2}]$, and $N(\pm\sqrt{-2}) = 2$, so $\sqrt{-2}$ is irreducible. Also $\sqrt{-2}$ divides $a + b\sqrt{-2}$ iff a is even. Similar argument as in the above paragraph will show that $\sqrt{-2}$ is a prime in $\mathbb{Z}[\sqrt{-2}]$. hence this is a decomposition into prime elements.

(b) For any $n > 2$, we first show that 2 is irreducible. For $2 = pq$ to be a non-trivial factrization, we must have $p, q \in \mathbb{Z}[\sqrt{-n}]$ with $N(p) = N(q) = 2$. But $N(p) = N(a + b\sqrt{-n}) = a^2 + b^2n = 2$ has no integer solutions a, b for $n \geq 2$, hence 2 is irreducible in $\mathbb{Z}[\sqrt{-n}]$.

Now we will show that 2 is not prime in $R = \mathbb{Z}[\sqrt{-n}]$ for any $n > 2$. If n is even, we have $\sqrt{-n}^2 = n$ is in $2R$, but $\sqrt{-n}$ is not in $2R$, hence 2 is not a prime. If n is odd, $(1 + \sqrt{-n})(1 - \sqrt{-n}) = 1 + n^2$ is in $2R$, but $1 \pm \sqrt{-n}$ are not in $2R$, so 2 is still not a prime.

(c) By (b), $\mathbb{Z}[\sqrt{-n}]$ can not be UFD for $n > 2$, but we know $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are UFD, hence 1 and 2 are the only number $n > 0$ such that $\mathbb{Z}[\sqrt{-n}]$ is a UFD. \square