20250124 MATH4302 Algebra II Assignment 1.

(1)

1) Proof: The number $1 \leq Char(R) \leq +\infty$ can be:

A. The number 1 B. A prime number $1 < p < +\infty$

C. A composite number $1 < c < +\infty$ D. The positive infinity $+\infty$

It suffices to disprove A and C.

For A, as R is not the zero ring, $0 \neq 1$ in R, so $Char(R) \neq 1$.

For C, assume to the contrary that $Char(R) = c_1 c_2$, where $c_1, c_2 \geq 2$. Then $c_1 \neq 0, c_2 \neq 0, c_1 c_2 = 0$ in R, so R contains a zero divisor.

2) Proof: We may divide our proof into two parts.

Field implies Integral Domain:

For all nonzero element r in the nonzero ring, r is a zero divisor implies $\exists s \in R \setminus \{0\}, rs = 0$.

Now for all $t \in R \setminus \{0\}$, rt cannot be 1, otherwise $s = rst = 0$.

Hence, r fails to be a unit, and the converse suggests our result.

Finite Integral Domain implies Field:

For all nonzero element r in the nonzero ring, as R is an integral domain, the translation map $f(s) = rs$ has an restriction on $R \setminus \{0\}$, and $\forall s, t \in R \setminus \{0\}$, $f(s) = f(t) \Rightarrow r(s-t) = 0 \Rightarrow s = t$, so f is injective.

As R is finite, f is surjective, $f(s) = 1$ has a solution, r is a unit, and R is a field.

Date / /

3). We may divide our proof into two parts.

$a|b \Rightarrow \langle a\rangle \supseteq \langle b\rangle$:

For all $r \in \langle b\rangle$, r is a multiple mb of b.

As $a|b$, b is a multiple na of a

Hence, r is a multiple mna of a, $r \in \langle a\rangle$, $\langle a\rangle \supseteq \langle b\rangle$

As a corollary, $a \sim b \Rightarrow \langle a\rangle = \langle b\rangle$.

In an integral domain, $\underset{\langle 0\rangle}{\overset{}{\langle a\rangle}} = \underset{\langle 0\rangle}{\overset{}{\langle b\rangle}} \Rightarrow a \sim b$:

$a \in \langle b\rangle \Rightarrow a$ is a multiple rb of b

$b \in \langle a\rangle \Rightarrow b$ is a multiple sa of a

$\Rightarrow a = rsa$

As R is an integral domain, cancel the nonzero factor a,

and we get $1 = rs$, so $a = rb \sim b$.

(2) We may divide our proof into two parts:

If S is a subring of an integral domain R, then S is an integral domain:

For all $s_1, s_2 \in S\setminus\{0_S\}$, $s_1, s_2 \in R\setminus\{0_R\}$, so $s_1s_2 \in R\setminus\{0_R\}$

As S is a subring, it is closed under multiplication, so $s_1s_2 \in S\setminus\{0_S\}$.

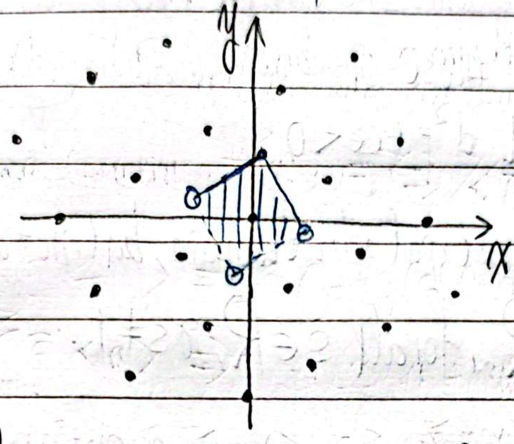
In the integral domain $\mathbb{Z}$, consider the nonprime ideal $4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.

(3) Define:

$$Deg: \mathbb{Z}[i]\setminus\{0\} \to \{1,2,3,\cdots\},\ Deg(m+ni)=m^2+n^2.$$

For all $a+bi\in\mathbb{Z}[i]$ and $c+di\in\mathbb{Z}[i]\setminus\{0\}$, consider:

$$\langle c+di\rangle = \{\lambda(c+di)+\mu(-d+ci) : \lambda,\mu\in\mathbb{Z}\}.$$



~~The following square generates a disjoint cover of $\mathbb{C}$:~~

$$(c+di)(-\tfrac{1}{2},\tfrac{1}{2}]+(-d+ci)(-\tfrac{1}{2},\tfrac{1}{2}]$$

Hence for every such combination, there exists a unique pair $p+qi,\ r+si\in\mathbb{Z}[i]$, such that:

$$a+bi=(p+qi)(c+di)+(r+si)$$

$$r+si\in(c+di)(-\tfrac{1}{2},\tfrac{1}{2}]+(-d+ci)(-\tfrac{1}{2},\tfrac{1}{2}]$$

$r+si=0$ or $Deg(r+si)=r^2+s^2\le\frac{1}{2}(c^2+d^2)<Deg(c+di)$

This means $\mathbb{Z}[i]$ is an Euclidean Domain.

(4) In $\mathbb{C}[t]$, all irreducible elements are exactly those linear polynomials $at+b$, where $a \neq 0$.

Hence, in $\mathbb{R}[t]$, every polynomial with no real root yields at least a pair of conjugate imaginary roots. As a consequence, all irreducible elements are exactly those linear polynomials $at+b$, where $a \neq 0$, and those irreducible quadratic polynomials ct^2+dt+e, where $c \neq 0$ and $d^2-4ce<0$

Prime ideal = Maximal ideal = Zero Ideal + Ideal generated by an irreducible

(5) As R is a principal ideal domain, but not a field, for some $r \in R$, for all $s \in R$, $rs \neq 1$.

Hence, $1 \notin \langle r, t \rangle$, so $\langle r, t \rangle$ is not principal, $R[t]$ is not a principal ideal domain.

(6) We apply the sieve of Eratosthenes.

Step 1: List all monic polynomials with $1 \leq \mathrm{Deg} \leq 3$:

t, $t+1$, $t+2$;

$\cancel{t^2}$, t^2+1, $\cancel{t^2+2}$, $\cancel{t^2+t}$, $\cancel{t^2+t+1}$, t^2+t+2, $\cancel{t^2+2t}$, $\cancel{t^2+2t+1}$, t^2+2t+2,

$\cancel{t^3}$, $\cancel{t^3+1}$, $\cancel{t^3+2}$, $\cancel{t^3+t}$, $\cancel{t^3+t+1}$, $\cancel{t^3+t+2}$, $\cancel{t^3+2t}$, t^3+2t+1, t^3+2t+2,

$\cancel{t^3+t^2}$, $\cancel{t^3+t^2+1}$, t^3+t^2+2, $\cancel{t^3+t^2+t}$, $\cancel{t^3+t^2+t+1}$, t^3+t^2+t+2, $\cancel{t^3+t^2+2t}$, t^3+t^2+2t+1, $\cancel{t^3+t^2+2t+2}$,

$\cancel{t^3+2t^2}$, t^3+2t^2+1, $\cancel{t^3+2t^2+2}$, $\cancel{t^3+2t^2+t}$, t^3+2t^2+t+1, $\cancel{t^3+2t^2+t+2}$, $\cancel{t^3+2t^2+2t}$, $\cancel{t^3+2t^2+2t+1}$, t^3+2t^2+2t+2.

Step 2: Cross out all multiples of t:

Step 3: Cross out all multiples of $t+1$:

Step 4: Cross out all multiples of $t+2$:

All irreducible quadratic polynomials: t^2+1, t^2+t+2, t^2+2t+2

All irreducible cubic polynomials: t^3+2t+1, t^3+2t+2, t^3+t^2+2, t^3+t^2+t+2, t^3+t^2+2t+1, t^3+2t^2+1, t^3+2t^2+t+1, t^3+2t^2+2t+2

(7) For all principal ideals $\{0\} \subsetneq \langle a \rangle, \langle b \rangle \subsetneq R$, consider the irreducible factorizations.

$$a = c_1^{s_1} c_2^{s_2} \cdots c_k^{s_k} \qquad b = c_1^{t_1} c_2^{t_2} \cdots c_k^{t_k}$$

Here, $c_1, c_2, \cdots, c_k$ are pairwisely distinct irreducible elements.

Define $c = c_1^{\max\{s_1,t_1\}} c_2^{\max\{s_2,t_2\}} \cdots c_k^{\max\{s_k,t_k\}}$.

This is a least common multiple of a, b

As c is a common multiple, $\langle c \rangle \subseteq \langle a \rangle \cap \langle b \rangle$.

As c is minimal, $\langle c \rangle \supseteq \langle a \rangle \cap \langle b \rangle$

(8) This proof is obtained from https://planetmath.org/equivalentdefinitionsforufd

We may divide our proof into two parts.

"if" direction: Assume to the contrary that R is not a unique factorization domain.

That is, for some $\alpha \in R$, $\alpha \neq 0$, α is nonunit, either α is never a product of irreducibles, or α can be written as different products of irreducibles.

In both cases, α is never a product of primes, because otherwise the product is always unique, and primes are irreducibles.

Consider the principal ideal $\langle \alpha \rangle$ generated by α,

and the set T of all products of primes, here all units are included.

Note that T is a subset with the property $\forall a, b \in R$, $ab \in T \Leftrightarrow a \in T$ and $b \in T$,

The intersection $\langle \alpha \rangle \cap T$ must be empty.

Consider the subset $A = \{I \text{ is an ideal of } R : I \cap T = \emptyset\}$.

As $\langle \alpha \rangle \in A$, and each totally ordered subset B of A has an upper bound $\bigcup_{I \in B} I \in A$, A contains a maximal element P. As $\{0\} \subsetneq \langle \alpha \rangle$, $P \neq \{0\}$.

I would like to prove that this P is prime in R.

We prove this by contradiction. Assume to the contrary that

$$x \notin P \Rightarrow (x)+P \supsetneq P \Rightarrow \exists\, a = \underset{\in P}{m} + \underset{\in (x)}{rx} \in [(x)+P]\cap T^c$$

$$y \notin P \Rightarrow (y)+P \supsetneq P \Rightarrow \exists\, b = \underset{\in P}{n} + \underset{\in (y)}{sy} \in [(y)+P]\cap T^c$$

$$xy \in P \Rightarrow ab = \overbrace{\underset{\in P}{m}\,\underset{\in P}{n}}^{\in P} + \overbrace{(\underset{\in R}{rx})\underset{\in P}{n}}^{\in P} + \overbrace{(\underset{\in R}{sy})\underset{\in P}{m}}^{\in P} + \overbrace{(\underset{\in R}{rs})(\underset{\in P}{xy})}^{\in P} \in P.$$

However, $a \in T^c$ and $b \in T^c \Rightarrow ab \in T^c \Rightarrow \underline{\underline{ab \in P \cap T^c = \emptyset}}$

Hence, P is prime in R, and this prime ideal $\underset{\neq\{0\}}{P} \subseteq T^c$ contains no prime element.

"only if" direction: Assume that R is a unique factorization domain.

For all nonzero prime ideal P of R, P contains a nonzero, nonunit element x. This x is a product $p_1p_2\cdots p_n$ of irreducibles, and it follows from the property of unique factorization domain that each irreducible is prime in R.

As $P \ni p_1p_2\cdots p_n$ is prime, P contains some prime p_k.

(9) Recall that a greatest common divisor b of B is an element of R with:

(1) b is a common divisor of B

(2) For all common divisor c of B, c divides b.

Assume that b_1, b_2 are two greatest common divisors of $B \subseteq R\setminus\{0\}$

As B contains a nonzero element, b_1, b_2 are nonzero.

As b_1, b_2 are maximal, $b_1 \mid b_2$ and $b_2 \mid b_1$, so $b_1 = ub_2 = b_1uv$.

This implies $uv = 1$ in the integral domain R, and b_1, b_2 are associated.

(10) Note that $\mathbb{Z}$ and $\mathbb{Q}[x]$ are unique factorization domains, so $\mathbb{Z}[x]$ is a unique factorization domain.

Factor $f(x) = 2x^2+2$, $g(x) = x^6-1$ into irreducibles:

$$f(x) = 2(x^2+1), \quad g(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

As $f(x), g(x)$ has no common irreducible factor, 1 is a greatest common factor of them.

Date / /