MA3201 Homework 3

Tan Yee Jian (A0190190L)

February 26, 2021

Problem 1

Let P be a prime ideal of a commutative ring R (with $1 \neq 0$). Let I, J be two ideals of R such that $I \cap J \subset P$. Prove that either $I \subset P$ or $J \subset P$.

Solution

Proof. For the sake of contradiction, suppose there is some $i \in I$ and $j \in J$ such that both are not in P. Then since both are in ideals, $ij \in I \cap J \subset P$. Since P is a prime ideal, we have $ij \in P \implies i \in P \vee j \in P$, a contradiction. □

Problem 2

Let $\mathbb{Z}[i]$ be the ring of Gaussian integers. Let $I \subset \mathbb{Z}[i]$ be a non-zero ideal. Prove that the quotient ring $\mathbb{Z}[i]/I$ is a finite set.

Solution

Recall that $\mathbb{Z}[i]$ is an Euclidean domain. Since it is in particular a principal ideal domain, let $I = (r)$. Then we carry out Euclidean division on any arbitrary element of R, say α, we have

$$\alpha = qr + \beta \qquad\qquad N(\beta) < N(r).$$

If $\beta = 0$, then $\alpha \in (r)$ is in the kernel. Otherwise $\beta > 0$, then there are only finitely many β such that $N(\beta) = a^2 + b^2 < N(r), \{a, b\} \subset \mathbb{Z}$. Therefore, its image under the quotient map must also be finite.

Problem 3

Let $p \in \mathbb{Z}$ be a positive prime. We define

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{Z}[x].$$

Prove that $\Phi_p(x)$ is irreducible.

Solution

Lemma. *Let R be a commutative ring. If $f(x) \in R[x]$ is reducible, then $f(x+1)$ is reducible.*

Proof of Lemma. Let $f(x) = a(x)b(x)$ where $a(x), b(x)$ are not units in $R[x]$. Then $a(x+1), b(x+1)$ cannot be units since their highest powers are preserved, according to the Binomial Theorem. Therefore $f(x+1) = a(x+1)b(x+1)$ witnesses the reducibility of $f(x+1)$. □

Now we use the contrapositive of the lemma to show that $\Phi_p(x+1)$ is irreducible, following the example on the textbook.

Proof of problem.

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1)-1} \\ &= \frac{1}{x}(x^p + px^{p-1} + \frac{p(p-1)}{2}x^{p-2} + \ldots + px + 1 - 1) \\ &= x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x^{p-3} + \ldots + p.\end{aligned}$$

Since $p \in \mathbb{Z}$ is prime, then all binomial coefficients of the form $\binom{p}{k}, 1 \leq k < p$ must be a multiple of p. By Eisenstein's criteria, $a^{p-1} = 0, a^{p-2}, \ldots, a^0 \in (p)$ but $a_0 = p \notin (p^2)$ gives us that $\Phi_p(x+1)$ is irreducible. By the contrapositive of the lemma above, $\Phi_p(x)$ must also be irreducible. □

Problem 4

Problem 4.1

Let R be an integral domain. Prove that the characteristic of R is a prime number or 0.

Solution

Proof. For the sake of contradiction, suppose the characteristic of R, c is positive but not a prime.

Case 1: $c = 1$
Then $1 = 0 \implies R$ is a trivial ring, $1 \times 1 = 0$ is a zero divisor, a contradiction.

Case 2: $\operatorname{char} R$ is composite
Then $c = ab$ for some $a, b \in \mathbb{N}$ where both a, b are not 1. Write $a_R = \sum^a 1_R, b_R \sum^b 1_R$, then we have

$$\begin{aligned}ab_R &= \underbrace{1_R + \ldots + 1_R}_{ab \text{ times}} \\ &= \overbrace{\underbrace{(1_R + \ldots + 1_R)}_{a \text{ times}} + \ldots + \underbrace{(1_R + \ldots + 1_R)}_{a \text{ times}}}^{b \text{ times}} \\ &= b_R \cdot a_R = 0_R.\end{aligned}$$

Both a_R, b_R cannot be 0_R since otherwise, it would be the characteristic of R. This means both are nonzero and thus are zero divisors, contradicting the integral domain assumption.

□

Problem 4.2

Let R be a field with $1 \neq 0$. Prove that the additive group R and the multiplicative group $R*$ are never isomorphic.

Solution

Proof. It is clear that R can never be finite, since otherwise, $|R| = |R^*| + 1$ cannot form a bijection.

We just consider the case where R is an infinite field. For the sake of contradiction, suppose $\phi : R \to R^*$ be an isomorphism. In particular, since it is a homomorphism, it must be that $\phi(0) = 1$. Let the characteristic of R be c, and we split by cases:

Case 1: $c = 2$
Then $1 + 1 = 0 \implies 1 = -1$. We have

$$\begin{aligned}\phi(1_R)^2 &= \phi(1_R) \cdot \phi(1_R) = \phi(1_R + 1_R) \\ &= \phi(0_R) && (1_R = -1_R \implies 2_R = 0_R) \\ &= 1_R && \text{(group homomorphisms preserve identity).}\end{aligned}$$

Solving the quadratic equation $x^2 = 1_R$ in R, we have $\phi(1_R) = 1_R$ uniquely (since the other solution $-1_R = 1_R$). This means $\phi(0_R) = \phi(1_R) = 1_R$, violating the bijectivity (in particular, injectivity) of ϕ. A contradiction.

Case 2: $c \neq 2$
Since ϕ is surjective, there exists some $x \in R$ such that $\phi(x) = -1_R \in R^*$. Then

$$\begin{aligned}
\phi(x) = -1_R &\implies \phi(x)^2 = (-1_R)^2 \\
&\implies \phi(2_R x) = 1_R \\
&\implies 2_R x = 0_R && \text{(since } \ker\phi = \{0_R\}) \\
&\implies x = 0_R && (\text{characteristic} \neq 2 \implies 2_R \neq 0_R) \\
&\implies \phi(x) = 1_R && \text{but } \phi(0_R) = 1_R.
\end{aligned}$$

Contradiction. ☐

Problem 5

Let R be an integral domain. Given R is an Artinian ring (thus fulfills the Descending Chain Condition), show that R is a field.

Solution

Proof. For any $0 \neq a \in R$, we can have a chain of ideals,

$$(a) \supseteq (a^2) \supseteq \cdots \supseteq (a^n) \supseteq \cdots$$

and there exists a $k \geq 1$ such that $(a^k) = (a^{k+1})$. We thus have a unit $b \in R$ such that

$$\begin{aligned}
a^k = ba^{k+1} &\implies a^k \cdot 1 = a^k(ab) && (\textit{commutative}) \\
&\implies ab = 1 && (a \neq 0,\ \text{integral domain}).
\end{aligned}$$

Therefore every non-zero element $a \in R$ is invertible $\implies$ R is a field. ☐