

Exercises on chapter 2

1. Let I be a proper ideal of a commutative ring R . Prove that I is maximal if and only if for every $a \in R - I$ there exists $b \in R$ such that $1 - ab \in I$.
2. Let R be a commutative ring, $R[X]$ be the polynomial ring in an indeterminate X with coefficients in R and $R[X][Y]$ be the polynomial ring in an indeterminate Y with coefficients in $R[X]$. Similarly define $R[Y][X]$, the polynomial ring in an indeterminate X with coefficients in $R[Y]$.
 - (i) Construct an isomorphism between $R[X][Y]$ and $R[Y][X]$. Henceforth, we denote this ring $R[X, Y]$ and call it the polynomial ring in indeterminates X and Y with coefficients in R . Similarly you can define $R[X_1, \dots, X_n]$ for n indeterminates $X_1, \dots, X_n \dots$
 - (ii) Prove that if F is a field then $F[X, Y]$ is not a PID.
3. Suppose that I and J are two-sided ideals of a ring R . Prove that $I \cap J$ and IJ are also two-sided ideals of R . (Remember the latter means the set of all sums $x_1y_1 + \dots + x_ny_n$ for $x_1, \dots, x_n \in I$ and $y_1, \dots, y_n \in J \dots$). Does $I \cap J = IJ$?
4. What is wrong with the following argument? The ring homomorphism $ev_{\sqrt{10}} : \mathbb{Z}[X] \rightarrow \mathbb{C}, f(X) \mapsto f(\sqrt{10})$ (“evaluation at $\sqrt{10}$ ”) has image $\mathbb{Z}[\sqrt{10}]$. Since $\mathbb{Z}[X]$ is a Euclidean domain it is a PID. Quotients of PIDs are PIDs. Hence $\mathbb{Z}[\sqrt{10}]$ is a PID.
5. Consider the ring $\mathbb{Z}[\sqrt{n}]$ for an integer n . There is a function $N : \mathbb{Z}[\sqrt{n}] \rightarrow \mathbb{Z}$ (called a “norm map”) defined by

$$N(a + b\sqrt{n}) = a^2 - nb^2.$$

(In the case of the Gaussian integers this is a degree function making $\mathbb{Z}[i]$ into a Euclidean domain.)

- (i) Verify that N is multiplicative, i.e. $N(xy) = N(x)N(y)$.
 - (ii) Prove that $x \in \mathbb{Z}[\sqrt{n}]$ is a unit if and only if $N(x) = \pm 1$. Hence determine the units in the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{10}]$.
 - (iii) If $x \in \mathbb{Z}[\sqrt{n}]$ has $N(x)$ a prime, show that x is irreducible.
 - (iv) Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{10}]$. Then use the observation that $2|6 = (4 + \sqrt{10})(4 - \sqrt{10})$ to prove that 2 is not a prime in $\mathbb{Z}[\sqrt{10}]$. Deduce that $\mathbb{Z}[\sqrt{10}]$ is not a PID (hence it is not an ED for any choice of degree function).
 - (v) Is $\mathbb{Z}[\sqrt{10}]$ a UFD?
6. This question is to make sure you haven’t forgotten how to calculate! If you don’t remember the Euclidean algorithm, look it up...
 - (i) Prove that the ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain with degree function $\phi(a + ib) = a^2 + b^2$.
 - (ii) Use the Euclidean algorithm to find the greatest common divisor of $16 + 7i$ and $10 - 5i$ in the ring $\mathbb{Z}[i]$. (You should also remember how to express this GCD as a linear combination

of the numbers you started with by working backwards through the algorithm, but I'm not going to make you do this... All this works in any Euclidean domain, e.g. \mathbb{Z} or $F[X]$ too.)

(iii) Express $27 + 6i$ as a product of primes in $\mathbb{Z}[i]$.

7. You might have seen this before but its rather pretty. Let p be an odd prime.

(i) If $p \equiv 1 \pmod{4}$, show that the polynomial $x^2 + 1$ has a root in \mathbb{Z}_p . Deduce that $x^2 + 1$ is reducible if $p \equiv 1 \pmod{4}$. (Hint: try $x = 1.2 \dots \frac{p-1}{2}$.)

(ii) Show that p is reducible in the ring $\mathbb{Z}[i]$ if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

(iii) Show that p is irreducible in the ring $\mathbb{Z}[i]$ if and only if $(x^2 + 1)$ is irreducible in the ring $\mathbb{Z}_p[x]$. (Hint: $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$.)

(iv) Show that if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ then $p \equiv 1 \pmod{4}$.

(v) Putting (i)–(iv) together, show that p can be written as a sum of two squares if and only if $p \equiv 1 \pmod{4}$.

8. A commutative ring is called a *local ring* if it has a unique maximal ideal.

(i) If p is prime, prove that the ring $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid p \nmid b\}$ is a local ring. (This is the localization of the ring \mathbb{Z} at the prime ideal (p) .)

(ii) If R is a local ring with unique maximal ideal \mathfrak{m} , prove that \mathfrak{m} is exactly the set of *non-units* in R .

9. (i) What are the maximal ideals of the ring \mathbb{Z}_{12} ?

(ii) Identify the ring \mathbb{Z}_{12} localized at the prime ideal (3) , i.e. what well known ring is $S^{-1}\mathbb{Z}_{12}$ where S is the multiplicative set $\{1, 2, 4, 5, 7, 8, 10, 11\}$ that is the complement of this prime ideal.

(iii) Identify the ring \mathbb{Z}_{12} localized at the prime ideal (2) .

10. Transitivity of localization. Let $S \subset T$ be two multiplicative sets in a commutative ring R . Let $i_S : R \rightarrow S^{-1}R$ be the localization of R at S . Let \bar{T} denote $\{i_S(t) \mid t \in T\} \subseteq S^{-1}R$ and $i_{\bar{T}} : S^{-1}R \rightarrow \bar{T}^{-1}(S^{-1}R)$ be the localization of $S^{-1}R$ at \bar{T} . Use the universal property of localization to prove that $i_{\bar{T}} \circ i_S : R \rightarrow \bar{T}^{-1}(S^{-1}R)$ is the localization of R at T .

11. Recall Eisenstein's criterion: let R be a UFD and $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. If there is some prime $p \in R$ such that $p \nmid a_n, p|a_i$ for $i = 0, \dots, n-1$ and $p^2 \nmid a_0$, then f is irreducible in $R[X]$.

(i) Prove that $X^3 + 3X^2 + 3X + 3$ is irreducible in $\mathbb{Q}[X]$.

(ii) Let p be a prime integer and

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

By substituting $X = Y + 1$ show that $\Phi_p(x)$ is irreducible.

12. This question is about cyclotomic polynomials. Let n be a positive integer. The n th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod (x - \omega)$$

where the product is over all primitive n th roots of unity $\omega \in \mathbb{C}$ (i.e. the $e^{2\pi im/n}$ for $m = 1, \dots, n-1$ with $(m, n) = 1$). So it is of degree $\phi(n)$ where ϕ is Euler's ϕ function (the number of units in \mathbb{Z}_n).

(i) Why is $x^n - 1 = \prod_{d|n} \Phi_d(x)$?

(ii) Using this prove by induction on n that $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$.

(iii) Compute $\Phi_p(x)$ for p prime.

(iv) Compute $\Phi_n(x)$ for $n \leq 12$. It is a theorem which I nearly made you prove in this exercise (but it was just too hard...) that $\Phi_n(x)$ is always irreducible.