

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 $1 - ab \in I$.

Say $I \subset J \subseteq R$ with $I \neq J$. We need to prove that $J = R$. Take $a \in J - I$. Then there exists $b \in R$ such that $1 - ab = c \in I$. Hence $1 = c + ab$ belongs to J . Hence $J = R$.

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.

(i) An element of $R[X][Y]$ looks like $\sum_j (\sum_i a_{i,j} X^i) Y^j$ for $a_{i,j} \in R$ all but finitely many of which are zero. An element of $R[Y][X]$ looks like $\sum_i (\sum_j a_{i,j} Y^j) X^i$. So the isomorphism is just “swap the summations”:

$$\sum_j \left(\sum_i a_{i,j} X^i \right) Y^j \mapsto \sum_i \left(\sum_j a_{i,j} Y^j \right) X^i.$$

(ii) Consider the ideal (X, Y) . Its a proper ideal, so doesn't contain any non-zero scalars (i.e. units). Suppose its principal, generated by a polynomial f . Note X is a multiple of f , say $X = fg$. Since X is irreducible hence prime, either f is X times a unit, or f is a unit, impossible as (X, Y) is proper. Similarly f is Y times a unit. Contradiction.

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 $x_1 y_1 + \dots + x_n y_n$ for $x_1, \dots, x_n \in I$ and $y_1, \dots, y_n \in J \dots$). Does $I \cap J = IJ$?

For $I \cap J$ its pretty obvious... For IJ , by definition it is a sub-abelian group. So we just need to check its “extra closed” under multiply on the left and on the right: take $x_1 y_1 + \dots + x_n y_n$ and any $a \in R$. Multiplying you get $(ax_1) y_1 + \dots + (ax_n) y_n$ which is in IJ as I is a left ideal. Similarly on the right as J is a right ideal. Hence its a two-sided ideal.

Its also clear that $IJ \subseteq I$ and $IJ \subseteq J$, hence $IJ \subseteq I \cap J$. The reverse inclusion is often true (e.g. its true in a PID), but in general it is false! Consider for example the ring $F[x, y]$, for F a field. Look at the ideals (x^2, y^3) and (x^3, y^2) . Their intersection is $(x^3, x^2 y^2, y^3)$. Their product is $(x^5, x^2 y^2, y^5)$. In particular y^3 lies in the intersection and not in the product.

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.

Well of course $\mathbb{Z}[X]$ is not a Euclidean domain. Its only polynomials over a field!

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?

(i) Yes it is (brute force).

(ii) If its a unit then $xy = 1$ for some y hence $N(xy) = N(x)N(y) = 1$ hence $N(x)$ is a unit in \mathbb{Z} hence $N(x) = \pm 1$.

Conversely, if $N(x) = \pm 1$, write $x = a + b\sqrt{n}$ and consider $y = (a - b\sqrt{n})/N(x)$. Then $xy = (a^2 - nb^2)/N(x) = 1$. Hence x is a unit.

(iii) Well if x is reducible then $x = ab$ where $N(a), N(b) \neq \pm 1$. Hence $N(x)$ factorizes hence it is not a prime. Its also all okay if x is zero or a unit...

(iv) $N(2) = 4$. So the only way that 2 could be reducible is if it factored as a product of things with norm 2. If $a^2 - 10b^2 = 2$ for integers a, b then reducing mod 5 you'd get that 2 was a quadratic residue mod 5 which its not. Hence 2 is irreducible.

Now suppose that 2 is prime. Since $2|(4 + \sqrt{10})(4 - \sqrt{10})$ it either divides $(4 + \sqrt{10})$ or $(4 - \sqrt{10})$. But each of these have norm 6 and 2 has norm 4 so that is impossible...

So we've found an irreducible that's not prime, it cannot be a PID.

(v) No. For instance $6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$ are two different ways of factoring 6 into irreducibles. Or remember that in any UFD primes and irreducibles are the same thing just like for PIDs...

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 $\mathbb{Z}[i]$.

(i) Let $w = a + ib$ be a Gaussian integer and $z = c + id$ be a non-zero Gaussian integer. Consider $w/z \in \mathbb{C}$. Think of it as a point somewhere on the complex plane, where the Gaussian integers are the lattice points with integer coordinates... The furthest a point can be from a lattice point is $\frac{\sqrt{2}}{2}$. So there exists a Gaussian integer $v = p + iq$ with $|v - w/z| \leq \frac{\sqrt{2}}{2} < 1$. In other words, $w = vz + u$ for a Gaussian integer u with $|u| = |w - vz| < |z|$. This gives a division algorithm for Gaussian integers proving that its a Euclidean domain...

(ii) Remember to find $GCD(a_1, a_2)$, you write $a_1 = a_2q + a_3$, $a_2 = a_3q + a_4, \dots$ until you get remainder zero. The remainder just before that is the GCD.

So

$$16 + 7i = (10 - 5i)(1 + i) + (1 + 2i)$$

then

$$(10 - 5i) = (1 + 2i)(-5i) + 0$$

So the GCD is $1 + 2i$.

(iii) Well, the norm of $27 + 6i$ (see the next problem) is 765 which factorizes as 5.9.17. Let me think of a Gaussian integer with norm 5 (automatically a prime). $1 - 2i$. Does it divide?

$$27 + 6i = (1 - 2i)(3 + 12i).$$

Now $(3 + 12i) = 3(1 + 4i)$ and $(1 + 4i)$ is prime as its norm is a prime. Finally we need to know if 3 is a prime... It is as its real and you can't write it as a sum of two squares. So the answer is $(1 - 2i)(1 + 4i)3$.

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 $p \equiv 1 \pmod{4}$.

(i) Take $x = 1.2 \dots \frac{p-1}{2}$. There are an even number of terms. So $x = (-1)(-2) \dots (-\frac{p-1}{2}) = (p-1)(p-2) \dots \frac{p+1}{2}$. Hence x^2 is the product of all numbers in \mathbb{Z}_p^\times . We need to show that this product is -1 . Well 1 and -1 are their own inverses, and their product is -1 . All the other elements split into pairs consisting of a number and its inverse, so their product is 1. Hence $x^2 + 1$ is reducible if $p \equiv 1 \pmod{4}$.

(ii) If $p = a^2 + b^2$ then $p = (a + ib)(a - ib)$ and its reducible. Conversely, suppose that p is reducible, say $p = (a + ib)(c + id)$. Since p is a prime integer we can't have $a = 0$ or $b = 0$. Then considering norms $p^2 = (a^2 + b^2)(c^2 + d^2)$. So $a^2 + b^2 = p = c^2 + d^2$.

(iii) p is irreducible in $\mathbb{Z}[i]$ if and only if $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(x^2 + 1, p) \cong \mathbb{Z}_p[x]/(x^2 + 1)$ is an integral domain if and only if $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$.

(iv) Say $p = a^2 + b^2$. One of a, b must be even, the other odd. Hence $p = (2c)^2 + (2d + 1)^2$ which is obviously $\equiv 1 \pmod{4}$.

(v) OKAY. So if p can be written as a sum of two squares its 1 mod 4 by (iv). Conversely, if p is 1 mod 4, then $x^2 + 1$ is reducible in $\mathbb{Z}_p[x]$ by (i), hence p is reducible in $\mathbb{Z}[i]$ by (iii), hence $p = a^2 + b^2$ by (ii).

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 .

(ii) Suppose that x is a non-unit not contained in \mathfrak{m} . Then (x) is a proper ideal of R not contained in \mathfrak{m} . By the existence of maximal ideals (proved in class using Zorn's lemma last term), we can embed x into a maximal ideal $M \neq \mathfrak{m}$. But that contradicts \mathfrak{m} being the unique maximal ideal of R .

(i) Let me show in general that if the set of non-units in R forms a proper ideal of R then R is a local ring. Well hang on that is obvious, since any proper ideal consists of non-units. So any proper ideal is certainly contained in the set of non-units in R .

Now look at $\mathbb{Z}_{(p)}$. Consider the set of units. Its all a/b with $p \nmid a$. Hence the non-units are all a/b with $p \mid a$. That is a proper ideal. So we've shown the set of all non-units forms a proper ideal so we're done by the preceding paragraph.

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).

(i) Its the same as the maximal ideals of \mathbb{Z} containing (12), i.e. the prime divisors of 12, i.e. (2) and (3).

(ii) Say $i : \mathbb{Z}_{12} \rightarrow R$ is the localization. Then $i(4)$ is a unit. But $i(4)i(3) = i(12) = 0$. Hence $i(3) = 0$ too. So (3) is contained in the kernel of the homomorphism i , and $\mathbb{Z}_{12}/(3) = \mathbb{Z}_3$. This suggests trying $R = \mathbb{Z}_3$ and i being reduction modulo 3. Note the images of the things in S are just 1 and 2, and these are indeed all units in \mathbb{Z}_3 .

Now let's check this satisfies the universal property of localization. Any map $f : \mathbb{Z}_{12} \rightarrow R$ mapping elements of S to units must map 3 to zero. Hence f factors through the quotient \mathbb{Z}_3 of \mathbb{Z}_{12} . We've checked it.

(iii) We need to localize at $S = \{1, 3, 5, 7, 9, 11\}$. So $i(3)$ is a unit. So $i(4) = 0$. So the localization might be \mathbb{Z}_4 , the map i being reduction modulo 4. The image of S is $\{1, 3\}$ which are units in \mathbb{Z}_4 . So yes that is it.

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 .

Take a ring homomorphism $f : R \rightarrow U$ such that $f(T) \subseteq U^\times$. In particular, $f(S) \subseteq U^\times$. Hence, by the universal property of i_S , there is a unique $\bar{f} : S^{-1}R \rightarrow U$ such that $f = \bar{f} \circ i_S$. So $\bar{f}(\bar{T}) = f(T) \subseteq U^\times$, hence by the universal property of $i_{\bar{T}}$, there is a unique $g : \bar{T}^{-1}(S^{-1}R) \rightarrow U$ such that $\bar{f} = g \circ i_{\bar{T}}$. Hence $f = g \circ i_{\bar{T}} \circ i_S$ which verifies that $i_{\bar{T}} \circ i_S : R \rightarrow \bar{T}^{-1}(S^{-1}R)$ has the universal property to be $T^{-1}R$..

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 $p \nmid a_n, p \mid a_i$ 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.

(i) I'll show its irreducible in $\mathbb{Z}[X]$, which is equivalent to it being irreducible in $\mathbb{Q}[X]$ by Gauss' lemma. Well apply Eisenstein with $p = 3$.

(ii) On substituting as hinted, you get

$$Y^{p-1} + \left(1 + \binom{p-1}{1}\right)Y^{p-2} + \dots + \left(1 + \binom{2}{1} + \dots + \binom{p-1}{p-2}\right)Y + p.$$

Simplifying using your favorite property of binomial coefficients this equals

$$Y^{p-1} + \binom{p}{1}Y^{p-2} + \binom{p}{2}Y^{p-3} + \dots + \binom{p}{p-1}Y + p.$$

All the coefficients except the first are divisible by p (think about it!) and the last one is not divisible by p^2 . So we're done by Eisenstein.

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.
- (i) Because $x^n - 1$ is $\prod (x - \omega)$ as ω runs over ALL n th roots of 1.
- (ii) We get from (i) that $x^n - 1 = f(x)\Phi_n(x)$ where by induction $f(x)$ is monic in $\mathbb{Z}[x]$. Hence by the division algorithm for polynomials, $\Phi_n(x)$ is monic in $\mathbb{Z}[x]$ too.
- (iii) If p is prime that $\Phi_p(x)$ is the product $\prod (x - \omega)$ for all p th roots of 1 except for $\omega = 1$ itself. Hence $\Phi_p(x) = (x^p - 1)/(x - 1)$ which is the polynomial listed in question 11.
- (iv) Just work inductively using (ii). Here goes...

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = x^2 - x + 1$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8(x) = x^4 + 1$$

$$\Phi_9(x) = x^6 + x^3 + 1$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{12}(x) = x^4 - x^2 + 1$$