

$R$  is a commutative ring with 1 and  $n \in \mathbb{N}_{>0}$ .

### ZAD. 1.

Let  $r_1, \dots, r_n \in R$ . Show that  $(r_1, \dots, r_n) = r_1R + \dots + r_nR$ .

From what I gathered,  $(r_1, \dots, r_n)$  is the minimal ring that contains  $\{r_1, \dots, r_n\}$ . Inclusion  $\subseteq$  is quite trivial but the other way around is more difficult.

Ok, so we need to have that for all  $r_i, r_j$  that  $r_i + r_j \in I$  so  $\sum r_i \in I$ . Furthermore, we need to have  $r_iR \in I$ . But that also means that  $r_iR + r_jR \in I$ , so we need to add all  $r_iR$  in order to obtain  $I$ . And I guess that is the end.

### ZAD. 2.

Let  $I \triangleleft R$  and  $\sqrt{I} := \{a \in R : (\exists n \in \mathbb{N}) a^n \in I\}$ . Show that  $\sqrt{I} \triangleleft R$ .

$I$  is an ideal, which means that  $a, b \in I \Rightarrow a + b \in I$  and  $r \in R, a \in I \Rightarrow ra \in I$ . This means that  $I$  is a normal subgroup of  $(R, +)$  and that notations starts to make sens to me right now.

First, let us tackle the multiplication. We take any  $a \in I$ . This means that for some  $n$   $a^n \in I$  and so for any  $r \in R$  we have  $ra^n \in I$ . So in particular for  $r^n \in R$  we have  $r^n a^n \in I$ , which means that  $r^n a^n = (ra)^n \in I$  and  $ra \in \sqrt{I}$  for any  $r \in R$ .

Now, for the addition. This one is more difficult because we have to see that for  $a^n, b^k \in I$  with assumption that  $k \leq n$  we also have  $(a + b)^n \in I$ . But if  $(a + b)^n \in I$  then in particular  $(a + b)^{2n} \in I$  and the other way around. So let us start here.

$$\begin{aligned}(a + b)^{2n} &= a^{2n} + \binom{2n}{1} a^{2n-1}b + \dots + \binom{2n}{2n-1} ab^{2n-1} + b^{2n} = \\ &= a^n(a^n + \binom{2n}{1} a^{n-1}b + \dots + \binom{2n}{n} b^n) + b^k(\binom{2n}{n-1} a^{n-1}b^{n+1-k} + \dots + \binom{2n}{1} ab^{2n-1-k} + b^{2n-k}) = \\ &= a^n \cdot r_a + b^k \cdot r_b\end{aligned}$$

for  $r_a, r_b \in R$  with those brutal formulas as seen above. Therefore  $a^n r_a \in I$  and  $b^k r_b \in I$  which means that  $a^n r_a + b^k r_b \in I$  but this is equal to  $(a + b)^n \in I$  so we have for  $a, b \in \sqrt{I}$   $a + b \in \sqrt{I}$ .

### ZAD. 3.

Let  $f : R \rightarrow S$  be a homomorphism of commutative rings with 1,  $I \triangleleft R$ , and  $J \triangleleft S$ . Show the following:

- $\hookrightarrow f^{-1}(J) \triangleleft R$
- $\hookrightarrow$  if  $f$  is an epimorphism (onto) then  $f(I) \triangleleft S$
- $\hookrightarrow$  give an example of  $f, I$  such that  $f(I) \not\triangleleft S$

$f^{-1}(J) \triangleleft R$

So let us take any  $a, b \in f^{-1}(J)$  we know that  $f(a), f(b) \in f(J)$  so  $f(a) + f(b) \in J$  as well. But  $f$  is a homomorphism, so it is additive or some bullshit and we can write

$$J \ni f(a) + f(b) = f(a + b)$$

so also  $a + b \in f^{-1}(J)$ , which gives as the addition thingy thing.

Now, the dreaded multiplication. We take any  $a \in f^{-1}(J)$  and any  $r \in R$ . We know that  $f(r) \in S$  and  $f(a) \in J$ , which means that  $f(r)f(a) \in J$ . But again,  $f$  is a homomorphism, so  $f(r)f(a) = f(ra) \in J$  so  $ra \in f^{-1}(J)$ .

$f(I) \triangleleft S$  when  $f$  is onto

First of all, addition. We know that  $a, b \in I$  implies that  $a + b \in I$ . So  $f(a) + f(b) = f(a + b) \in f(I)$ . Now, for the multiplication. We take any  $r \in R$  and any  $a \in I$  and we know that  $ra \in I$  so  $f(ra) = f(r)f(a) \in f(I)$  and  $f(r)$  can be any element in  $S$  because  $f$  is onto.

EXAMPLE but im too lazy to think about it right now.

## ZAD. 4.

Find  $f \in \mathbb{Q}[X]$  such that  $(f) = (X^2 - 1, X^3 + 1)$ .

So we are looking for a function for which the smallest ideal that contains it is equal to the smallest ideal that contains  $X^2 - 1$  and  $X^3 - 1$ . Maybe first let us write down how the RHS looks like

$$(X^2 - 1, X^3 - 1) = \{ra : r \in \mathbb{Q}[X], a = X^2 - 1, X^3 + 1\}.$$

Ok, now how about the LHS?

$$(f) = \{rf : r \in \mathbb{Q}[X]\}$$

Let us take any  $r \in \mathbb{Q}[X]$  then we have  $r(X^2 - 1) \in (f)$  and  $r(X^3 - 1) \in (f)$ . Furthermore, we have that  $(X^2 - 1) + (X^3 - 1) = X^3 + X^2 \in (f)$ . Maybe  $f = X + 1$ ? Yep.

We have that

$$(X + 1)(X - 1) = X^2 - 1 \in \text{RHS}$$

and also

$$(X^2 - X + 1)(X + 1) = X^3 + 1 \in \text{RHS}$$

$$X^2(X + 1) = X^3 + X^2 \in \text{RHS}$$

## ZAD. 5.

Show that the ideal  $(2, X) \triangleleft \mathbb{Z}[X]$  is not principal.

A principal ideal is an ideal  $I$  generated by one element  $a \in R$  through multiplication of  $a$  by all elements of  $R$ .

$$(2, X) = \{ra : r \in \mathbb{Z}[X], a = 2, X\}$$

So what if  $(2, X)$  was a principal ideal? We would have an  $a \in \mathbb{Z}[X]$  such that

$$(\forall y \in (2, X))(\exists r \in \mathbb{Z}[X]) \quad ra = y$$

So let us start with 2 and  $X$ . We assumed that  $a$  as above existed, so

$$r_1 \cdot a = 2$$

$$r_2 \cdot a = X$$

and then

$$2 + X = r_1 \cdot a + r_2 \cdot a = (r_1 + r_2) \cdot a.$$

Now, because we only have polynomials with integer coefficients, we must have  $a$  of order 0, otherwise we could not obtain 2 by multiplying  $a$  by some other polynomial. We can have either  $a = 1$  or  $a = 2$ . So for the second case we would need to find  $r_2$  such that  $r_2 \cdot 2 = X$  and we know that  $r_2$  must be of order 1 so it must be  $r_2 = r'_2 X$  and  $r'_2 X \cdot 2 = X$  meaning, that  $r'_2 = \frac{1}{2}$  which cannot be. Therefore, we are left with  $a = 1$  and  $r_2 = 2$ . Then, we have

$$2 + X = 2 \cdot 1 + X \cdot 1 = (2 + X) \cdot 2 = 4 + 2X$$

and this is a contradiction.