

393 HOMEWORK 3 SOLUTIONS

• Exercises 5.1: 21, 23.

21 Let V and W be vector spaces over a field F and $T : V \rightarrow W$ be a linear transformation. Prove that

- (a) $\ker T$ is a subspace of V .
- (b) $\operatorname{im} T$ is a subspace of W .
- (c) For any subspace U of V , $T(U)$ is a subspace of W .
- (d) For any subspace Z of W , $T^{-1}(Z)$ is a subspace of V .

Solution. Note (b) follows from (c) taking the special case $U = V$, and (a) follows from (d) taking the special case $Z = \{0\}$. So I just need to prove (c) and (d).

(c) We need to show $T(U)$ is closed under addition and under scalars. I'll just do the closed under addition part. Take two vectors, $T(u), T(u') \in T(U)$, for $u, u' \in U$. Then $T(u) + T(u') = T(u + u')$. Since U is a subspace, $u + u' \in U$. Hence, $T(u + u') \in T(U)$.

(d) We need to show $T^{-1}(Z)$ is closed under addition and under scalars. I'll just do the closed under scalars part. Take a vector $v \in T^{-1}(Z)$ and a scalar c . So $T(v) \in Z$. We need to show that $cv \in T^{-1}(Z)$, i.e. that $T(cv) \in Z$ too. But $T(cv) = cT(v)$ and $T(v) \in Z$ which is a subspace, so $cT(v) \in Z$, done.

23 Let V be a finite dimensional vector space and $T : V \rightarrow W$ be a linear transformation.

- (a) Suppose $\ker T = \{0\}$. Show that if $v_1, \dots, v_k \in V$ are linearly independent, so are $T(v_1), \dots, T(v_k) \in W$.
- (b) More generally, let u_1, \dots, u_l be a basis for $\ker T$ and extend to a basis $u_1, \dots, u_l, v_1, \dots, v_k$ for V . Prove that $T(v_1), \dots, T(v_k)$ is a basis for $\operatorname{im} T$.
- (c) Prove that $\dim V = \dim \ker T + \dim \operatorname{im} T$.

Solution. Since (a) is a special case of (b), I'll skip the proof of (a). For (b), we show $T(v_1), \dots, T(v_k)$ span $\operatorname{im} T$ and that they are linearly independent.

SPAN: any vector of $\operatorname{im} T$ looks like $T(a_1u_1 + \dots + a_lu_l + b_1v_1 + \dots + b_kv_k)$ since the u 's and the v 's span V . Since T is a linear transformation and $T(u_1) = \dots = T(u_l) = 0$ this equals $b_1T(v_1) + \dots + b_kT(v_k)$. Hence any vector of $\operatorname{im} T$ is a linear combination of $T(v_1), \dots, T(v_k)$ as required.

LINEARLY INDEPENDENT: Suppose $b_1T(v_1) + \dots + b_kT(v_k) = 0$. We need to show that $b_1 = \dots = b_k = 0$ already. Well, since T is linear, we have that $T(b_1v_1 + \dots + b_kv_k) = 0$. Hence $b_1v_1 + \dots + b_kv_k$ lies in $\ker T$, so it is a linear combination $a_1u_1 + \dots + a_lu_l$ of our basis for $\ker T$. Hence, $b_1v_1 + \dots + b_kv_k - a_1u_1 - \dots - a_lu_l = 0$. Since the v 's and the u 's are

linearly independent, this implies the coefficients b_1, \dots, b_k are zero, as required.

• Exercises 5.2: 10, 13.

10 (a) Prove that if the regular mn -gon is constructible, so is the regular m -gon and the regular n -gon.

(b) Prove that if $\text{GCD}(m, n) = 1$ and the regular m and n -gons are constructible, so is the regular mn -gon.

Solution. (a) Since the regular mn -gon is constructible, we can construct the angle $360/mn$. Constructing it m times next to each other gives the angle $m(360/mn) = 360/n$. Hence the regular n -gon is constructible. Similarly for m .

(b) Since $\text{GCD}(m, n) = 1$, we can write $1 = am + bn$ for $a, b \in \mathbb{Z}$. Since the regular m and n -gons are constructible, we can construct the angles $360/m$ and $360/n$. Hence we can construct the angles $b(360/m)$ and $a(360/n)$, hence their sum

$$b(360/m) + a(360/n) = 360((am + bn)/mn) = 360/mn.$$

Hence we can construct the regular mn -gon.

13 Show an angle of 3 degrees is constructible, whereas an angle of 1 degree is not. Now decide which angles n degrees are constructible for $n \in \mathbb{Z}$.

Solution. We have seen how to construct the regular 3-gon and the regular 5-gon, hence the angles 60 degrees and 72 degrees. Their difference gives us a construction of the angle 12 degrees. Bisecting this angle twice gives us 3 degrees.

To see 1 degree is not constructible, suppose for a contradiction that it is. Doing it 20 times in a row gives us a construction of the angle 20 degrees. But we proved in class that the angle 20 degrees is not constructible, contradiction.

Hence the angle n degrees is constructible if and only if $3|n$. For since we can construct 3 degrees, we can construct any multiple of 3 degrees. On the other hand, if we could construct n degrees for n not a multiple of 3, then since $\text{GCD}(n, 3) = 1$ and we can write $1 = an + 3b$ for integers a, b we could construct the angle 1 degree too, which we cannot!

• Exercises 5.3: 2, 3, 4.

2 Construct explicitly a field with 32 elements.

Solution. We need to find a monic polynomial $f(x)$ of degree 5 that is irreducible in $\mathbb{Z}_2[x]$. Then $\mathbb{Z}_2[x]/(f(x))$ will be a field with 32 elements.

We obviously must only think about the candidates that don't have 0 or 1 as a root. Moreover, if a poly of degree 5 is reducible without linear factors, it must have an irreducible quadratic factor, and the only irreducible quadratic is $x^2 + x + 1$. So we want

to ensure our candidate is also not divisible by $x^2 + x + 1$, then it will for sure be irreducible.

Try $x^5 + x^2 + 1$.

- 3 The polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$ so $K = \mathbb{Z}_3[x]/(x^2 + 1)$ is a field with nine elements. Let $\alpha \in K$ be a root of $f(x)$. Find irreducible polynomials in $\mathbb{Z}_3[x]$ having roots (a) $\alpha + 1$ (b) $\alpha - 1$.

It might be more suggestive to write i instead of α for the root of $f(x)$: the field K is really just the field $\mathbb{Z}_3[i]$ with a “square root of -1 ” adjoined.

Say $x = i + 1$. Then, $(x - 1) = i$ so $(x - 1)^2 = -1$ so $x^2 - 2x + 2 = 0$. So $i + 1$ is a root of the polynomial $x^2 + x + 2 \in \mathbb{Z}_3[x]$, which is easy to see is irreducible since it has no roots.

Say $x = i - 1$. Then, $(x + 1) = i$ so $(x + 1)^2 = -1$ so $x^2 + 2x + 2 = 0$. So $i - 1$ is a root of the polynomial $x^2 + 2x + 2$, again irreducible.

- 4 Construct explicitly an isomorphism

$$\mathbb{Z}_2[x]/(x^3 + x + 1) \rightarrow \mathbb{Z}_2[x]/(x^3 + x^2 + 1).$$

Solution. Let $R = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$. We know for each $\alpha \in R$ that there is a homomorphism ev_α

$$\mathbb{Z}_2[x] \rightarrow R$$

sending a polynomial $f(x) \in \mathbb{Z}_2[x]$ to the number $f(\alpha) \in R$. I want to pick α so that ev_α is onto and its kernel is $(x^3 + x + 1)$. Then it will induce an isomorphism $\mathbb{Z}_2[x]/(x^3 + x + 1) \rightarrow R$ and we’ll be done.

So we need to find $\alpha \in R$ such that $\alpha^3 + \alpha + 1 = 0$. A little trial and error gives that $\alpha = \overline{x + 1}$ works:

$$\begin{aligned} \alpha^3 + \alpha + 1 &= (x + 1)^3 + (x + 1) + 1 = x^3 + 3x^2 + 3x + 1 + x + 1 + 1 = \\ &= x^2 + 1 + 3x^2 + 3x + 1 + x + 1 + 1 = 0. \end{aligned}$$

Now we’re done. The isomorphism

$$\mathbb{Z}_2[x]/(x^3 + x + 1) \rightarrow \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$$

is given explicitly by the map sending $f(x) \in \mathbb{Z}_2[x]/(x^3 + x + 1)$ to $f(x + 1) \in \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$.