December 2020

Practice Problem Set – Solutions

Exercise 1. *For each of the following statements, determine if it is true or false. Justify your answer by a proof or a counter-example.*

(a) There are no nontrivial zero divisors in a field.

(b) Every element of a field is irreducible.

(c) In a ring R the element 1_R is always irreducible.

(d) Let K be a field. The polynomial ring $K[X]$ is a principal ideal domain.

(e) In a principal ideal domain any irreducible element generates a maximal ideal.

(f) The ring $\mathbb{Z}$ is a principal ideal domain.

(g) The ring $\mathbb{Z}[X]$ is a principal ideal domain.

(h) In the ring $\mathbb{Z}$ any irreducible element is positive.

Solution 1. (a) The statement is true. Suppose x, y are elements in a field K such that $xy = 0$. If $x \neq 0$, then x^{-1} exists. Multiply x^{-1} to both sides of $xy = 0$, so we have that $y = 0$.

(b) The statement is false. The set of the irreducible elements of a field is empty. By definition an irreducible element of a ring R is a non-zero, non-unit element that is not reducible. But in a field the set of non-zero, non-unit elements is exactly the empty set.

(c) The statement is false. The element 1_R belongs to R^*, thus it cannot be an irreducible element.

(d) The statement is true. The ring of polynomials in one variable with coefficients over a field K is a euclidean ring therefore by the theorem of the course it is a principal ideal domain.

(e) The statement is true. In a PID, an element p is irreducible if and only if the ideal (p) is maximal. (See lecture notes alg-2019-12.pdf).

(f) This statement is true. In fact $\mathbb{Z}$ is a Euclidean domain, since the Euclidean algorithm works in it, and therefore it is also a PID.

(g) This statement is false. Consider the ideal I generated by $\{X, 2\}$ in $\mathbb{Z}[X]$. Suppose there is a polynomial $f(X)$ that generates this ideal. Then $2 = g(X)f(X)$, and therefore the degree of $f(X)$ and $g(X)$ is zero. Since the ideal I is proper, $1 \notin I$ and $f(x) = \pm 2$. Also $X = h(X)f(X) = \pm 2h(X)$, which is impossible for $h(X) \in \mathbb{Z}[X]$. Therefore $\mathbb{Z}[X]$ is not a PID.

(h) The statement is false. Observe that -5 is a non-zero, non-unit element that can be written only as $-5 = -1 \cdot 5$ or $-5 = 1 \cdot (-5)$. This is an irreducible element, since ± 1 are units.

Exercise 2. *Consider the ideals $I = 24\mathbb{Z}$, $J = 30\mathbb{Z}$, $K = 9\mathbb{Z}$, $L = 3\mathbb{Z}$ and $M = 7\mathbb{Z}$ in the ring $\mathbb{Z}$. For each of the following ideals find $m \in \mathbb{Z}$ such that the given ideal is equal to $(m) = m\mathbb{Z} \in \mathbb{Z}$.*

$$I + J,\ I \cap J,\ I + J + L,\ I + M,\ I \cap L,\ \ J + I + M,\ , IJ \cap K.$$

Do the same for the ring $\mathbb{R}[X]$ and the ideals $L = (X-1)$, $K = (X+1)$, $M = (X^2+1)$, $I = (X^2-X)$ et $J = (X^4-1)$.

Solution 2. Recall that if R is a principal ideal domain and a, $b \in R$, then

$$(m) = (a) \cap (b) \quad (d) = (a) + (b) \quad \text{and} \quad (ab) = (a)(b)$$

where $m = \text{lcm}(a, b)$ and $d = \gcd(a, b)$. (Here the abbreviation "lcm" is for "least common multiple" which is the ppcm.)
Then, since $\mathbb{Z}$ and $\mathbb{R}[X]$ are principal ideal domain, we have that:

- $24\mathbb{Z}+30\mathbb{Z}=6\mathbb{Z}$, $24\mathbb{Z}\cap 30\mathbb{Z}=120\mathbb{Z}$, $24\mathbb{Z}+30\mathbb{Z}+3\mathbb{Z}=3\mathbb{Z}$, $24\mathbb{Z}+7\mathbb{Z}=\mathbb{Z}$, $24\mathbb{Z}\cap 3\mathbb{Z}=24\mathbb{Z}$, $24\mathbb{Z}+30\mathbb{Z}+7\mathbb{Z}=\mathbb{Z}$ and $(24\mathbb{Z})(30\mathbb{Z})\cap 9\mathbb{Z}=720\mathbb{Z}$.
- $I+J=(X-1)$, $I\cap J=(X(X^4-1))$, $I+J+L=(X-1)$, $I+M=\mathbb{R}[X]$, $I\cap L=(X^2-X)$, $J+I+M=\mathbb{R}[X]$, $IJ\cap K=(X^6-X^5-X^2+X)$

Exercise 3. *Show that the ideal $I=(2,X)$ in the ring $\mathbb{Z}[X]$ is not principal. Describe the ideal $I=(2,X)$ in the ring $\mathbb{Q}[X]$.*

Solution 3. Assume that the ideal $(2,X)\subseteq\mathbb{Z}[X]$ is generated by a single element $P\in\mathbb{Z}[X]$, i.e. $(2,X)=(P)$. Then, since $2,X\in(P)$, we can find $Q,Q'\in\mathbb{Z}[X]$ with $2=PQ$ and $X=PQ'$.

Since $0=\deg(2)=\deg P+\deg Q$, (since $\mathbb{Z}$ is an integral domain), P must be a polynomial of degree 0, i.e. a constant non-zero polynomial aX^0 for some $a\in\mathbb{Z}\setminus\{0\}$. Similarly, since $1=\deg X=\deg P+\deg Q'=\deg Q'$, Q' must be of the form $bX+c$ for $b,c\in\mathbb{Z}$. Thus we obtain $X=PQ'=a(bX+c)=(ab)X+ac$. In particular, $ab=1$, so $a\in\{1,-1\}$.

Now we have $aX^0=P\in(2,X)$ by our assumption $(2,X)=(P)$, so we can find $T,U\in\mathbb{Z}[X]$ s.t. $aX^0=X\cdot T+2\cdot U$. Let $u_0\in\mathbb{Z}$ be the constant coefficient of U. Then, by the equation above, we have $a=2u_0$ since $X\cdot T$ contains only terms of positive degree. This yields a contradiction since $a\in\{1,-1\}$ cannot be a multiple of 2. Hence the assumption is false and $(2,X)\subseteq\mathbb{Z}[X]$ is not a principal ideal.

In the ring $\mathbb{Q}[X]$, the ideal generated by 2 and X is in fact the whole ring: We can write $1_{\mathbb{Q}[X]}$ as $X\cdot 0+2\cdot\frac{1}{2}$, so $1\in(2,X)_{\mathbb{Q}[X]}$. Then for all $P\in\mathbb{Q}[X]$, we have $P=P\cdot 1\in(2,X)_{\mathbb{Q}[X]}$ since $(2,X)_{\mathbb{Q}[X]}$ is an ideal. Hence $(2,X)_{\mathbb{Q}[X]}=\mathbb{Q}[X]=(1)_{\mathbb{Q}[X]}$ is a principal ideal.

Exercise 4. *Let A and B be two rings, $U(A)\subset A$ and $U(B)\subset B$ the groups of invertible elements and $\Phi:A\to B$ a ring homomorphism.*

(a) Show that the set $\Phi(U(A))$ is a subgroup of $U(B)$.

(b) Suppose that $\Phi:A\to B$ is surjective. Is it always true that $\Phi(U(A))=U(B)$? Hint: consider the case $A=\mathbb{Z}$, $B=\mathbb{Z}/7\mathbb{Z}$ and $\Phi(k)=[k]_7$ for all $k\in\mathbb{Z}$.

Solution 4. (a) If $x,y\in U(A)$, then $\Phi(x)\Phi(y)=\Phi(xy)\in\Phi(U(A))$, $\Phi(1_A)=1_B$ and $\Phi(x)\Phi(x^{-1})=1_B$, therefore $\Phi(U(A))\subset U(B)$ is closed with respect to products and taking inverses, contains the neutral element, and is a subgroup.

(b) If $\Phi:A\to B$ is surjective, this does not imply that $\Phi(U(A))=\Phi(U(B))$. In particular, for any prime $p\in\mathbb{Z}$, we have $\Phi:\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$ is the unique ring homomorphism, that is surjective. However, $U(\mathbb{Z})=\{\pm 1\}$ and $U(\mathbb{Z}/p\mathbb{Z})=\{[1]_p,[2]_p,\dots[p-1]_p\}$, so $\Phi:U(\mathbb{Z})\to U(\mathbb{Z}/p\mathbb{Z})$ is not surjective for any prime $p>3$.

Exercise 5. *Let $\Phi_1:\mathbb{Z}/11\mathbb{Z}\to A$ and $\Phi_2:\mathbb{Z}/15\mathbb{Z}\to B$ be ring homomorphisms. What can be the number of elements in the image of Φ_1 (respectively Φ_2)?*

Solution 5. The kernel of a ring homomorphism is an ideal in the ring. There are only two ideals, $\mathbb{Z}/11\mathbb{Z}$ and $\{0\}$ in the ring $\mathbb{Z}/11\mathbb{Z}$. In addition, by definition of a ring homomorphism, $\Phi(1)=1$ and therefore the entire ring cannot be in the kernel of Φ. Then the only choice for the kernel of Φ_1 is the trivial ideal $\{0\}$, and the image is isomorphic to the whole ring $\mathbb{Z}/11\mathbb{Z}$, containing 11 elements.
The kernel of Φ_2 can be equal to any of the the ideals $(0)\in\mathbb{Z}/15\mathbb{Z}$, $(3)\in\mathbb{Z}/15\mathbb{Z}$ or $(5)\in\mathbb{Z}/15\mathbb{Z}$. Respectively, the number of elements in the image can be 15, 3 or 5.

Exercise 6. *(a) Find the characteristic of the polynomial rings $\mathbb{Z}[x]$, $\mathbb{R}[x]$ et $\mathbb{F}_p[x]$.*

(b) Find the order and the characteristic of $\mathbb{F}_2[x]/I$, where I is generated by the ideal x^3-1.

Solution 6. (a) Since the image of 1 under the unique ring homomorphism $\phi:\mathbb{Z}\to A$ is 1, and we have that $n\cdot 1\neq 0$ in $\mathbb{Z}[x]$ and in $\mathbb{R}[x]$, the characteristic of these rings is 0. We have $p\cdot 1=0\in\mathbb{Z}/p\mathbb{Z}$, and therefore $(p)=\ker\phi:\mathbb{Z}\to\mathbb{F}_p[x]$, and the characteristic of $\mathbb{F}_p[x]$ is p.

(b) We have $x^3-1=(x-1)(x^2+x+1)\in\mathbb{F}_2[x]$ the factorization of the polynomial x^3-1 into irreducibles over $\mathbb{F}_2$. Since the polynomials $x-1,x^2+x+1$ are coprime, we have by the Chinese remainder theorem:

$$\mathbb{F}_2[x]/(x^3-1)\simeq\mathbb{F}_2[x]/(x-1)\times\mathbb{F}_2[x]/(x^2+x+1)=A\times B.$$

We have $A = \mathbb{F}_2[x]/(x-1) \simeq \mathbb{F}_2$ with order $|A| = 2$ and the characteristic $c_A = 2$. Also, $B = \mathbb{F}_2[x]/(x^2+x+1)$ is a field, and $|B| = 4$ since x^2+x+1 is irreducible polynomial of order 2 over $\mathbb{F}_2$. Its characteristic is equal to the characteristic of $\mathbb{F}_2[x]$, which is 2. The number of elements in $A \times B$ is $|A \times B| = |A||B| = 8$. By Exercise 3, PS11, we have that the characteristic of a direct product is the least common multiple of the characteristics of the two rings. Therefore, $c_{A\times B} = \mathrm{lcm}(2,2) = 2$.

Exercise 7. *(a) Find the monic greatest common divisor of the polynomials $2x^3 - 11x^2 + 2x - 11$ and x^2+1 in $\mathbb{Q}[x]$.*

(b) Are the polynomials $h_1(x) = x^3 - 2x^2 - x - 18$ and $h_2(x) = x^2 - 5x - 6$ coprime in $\mathbb{Q}[x]$?

(c) Which of the polynomials $f_1(x) = x^3+1$, $f_2(x) = x^3+x^2+1$, $f_3(x) = x^3+x^2+x+1$ are irreducible in $\mathbb{F}_2[x]$? Give the factorization into irreducible factors for those that are not irreducible.

(d) Are the polynomials $g_1(x) = x^2 - 2$ and $g_2(x) = x^2 - 3$ irreducible in $\mathbb{Q}[x]$? in $\mathbb{F}_{11}[x]$?

Solution 7. (a) We have $2x^3 - 11x^2 + 2x - 11 = (x^2+1)(2x-11)$, therefore the monic polynomial x^2+1 is the $\gcd(2x^3 - 11x^2 + 2x - 11, x^2+1)$ in $\mathbb{Q}[x]$.

(b) We have $h_2(x) = x^2 - 5x - 6 = (x-6)(x+1)$. Since $h_1(-1) < 0$ and $h_1(6) > 0$, the the elements $h_1(x)$ and $h_2(x)$ are coprime in $\mathbb{Q}[x]$.

(c) Since the given polynomials are of degree 3, it suffices to check if they have roots in $\mathbb{F}_2$. We have $f_1(0) = 1, f_1(1) = 0$, $f_2(0) = 1, f_2(1) = 1$, $f_3(0) = 1, f_3(1) = 0$. Therefore only $f_2(x)$ is irreducible in $\mathbb{F}_2[x]$. For other polynomials, we have $f_1(x) = (x+1)(x^2+x+1)$, $f_3(x) = (x+1)^3$.

(d) Again, since the polynomials are of degree 2, it suffices to check for the roots. We have that $g_1(x)$ and $g_2(x)$ have no roots in $\mathbb{Q}$, and therefore they are irreducible in $\mathbb{Q}[x]$. In $\mathbb{F}_{11}$ we have: $2^2 = 4, 3^2 = 9, 4^2 = 5, 5^2 = 3, 6^2 = 3, 7^2 = 5, 8^2 = 9, 9^2 = 4, 10^2 = 1$. Therefore the poynomial $g_2(x) = x^2 - 3 = (x-5)(x-6)$ is not irreducible, but $g_1(x) = x^2 - 2$ is irreducible in $\mathbb{F}_{11}[x]$.

Exercise 8. *(a) Show that the fields $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{5}]$ are not isomorphic.*

(b) Show that the rings $\mathbb{F}_5[x]/(x^2-2)$ are $\mathbb{F}_5[x]/(x^2-3)$ are fields. Are they isomorphic?

(c) Find an explicit isormophism between the fields $\mathbb{R}[x]/(x^2-2x+2)$ and $\mathbb{R}[x]/(x^2+1)$.

Solution 8. (a) Suppose there exists an isomorphism $f : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{5}]$. Then we must have $f(1) = 1$, and therefore $f(3) = 3$. Let $f(\sqrt{3}) = a + b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ for some $a, b \in \mathbb{Q}$. Then $f(\sqrt{3})^2 = f(3) = 3 = a^2 + 2ab\sqrt{5} + 5b^2$. Then either $a = 0$, or $b = 0$. If $b = 0$, then $a^2 = 3$, which is impossible for an $a \in \mathbb{Q}$. If $a = 0$, then $5b^2 = 3$, say $b = \frac{r}{s}$ for integers $r, s \in \mathbb{Z}$ with $\gcd(r,s) = 1$. Then $5r^2 = 3s^2$, so $r = 3k$ and $s = 5m$, so we have $45k^2 = 75m^2$, or $3k^2 = 5m^2$. Repeating the same argument, we get $k = 5u, m = 3v$, and $5u^2 = 3v^2$, where $\frac{r}{s} = \frac{3k}{5m} = \frac{15u}{15v} = \frac{u}{v}$, which contradicts the choice of $r, s \in \mathbb{Z}$ such that $\gcd(r,s) = 1$. Therefore no isomorphism between the fields $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{5}]$ is possible.
Note that the argument works as well for any pair of distinct primes $p \neq q$: $\mathbb{Q}[\sqrt{p}] \neq \mathbb{Q}[\sqrt{q}]$.

(b) The polynomials $x^2 - 2$ and $x^2 - 3$ are irreducible over $\mathbb{F}_5$, since they have no roots in $\mathbb{F}_5$. Indeed, $1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1$ in $\mathbb{F}_5$. Since according to theorem from the course there exists a unique field of 5^2 elements up to isomorphism, these fields are isomorphic.

(c) We have the congruence class of $\pm x$ in $\mathbb{R}[x]/(x^2+1)$ are square roots of -1, therefore they can be denoted $\pm i$ and the field is isomorphic to $\mathbb{C}$. In the other ring we have $(x-1-i)(x-1+i) = x^2 - 2x + 2$. Therefore $f : [x]_{(x^2-2x+2)} \mapsto 1 + [x]_{(x^2+1)}$ defines a field isomorphism $R[x]/(x^2-2x+2) \to \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Exercise 9. *Give examples of fields of 25 and 27 elements.*

Solution 9. By theorems from the course, It suffices to find an irreducible polynomial of degree 2 over $\mathbb{F}_5$ and of degree 3 over $\mathbb{F}_3$. For example, we have $x^2 - 2$ is irreducible over $\mathbb{F}_5$ (since $a^2 \neq 2$ for any $a \in \mathbb{F}_5$), and the field $\mathbb{F}_5[x]/(x^2-2)$ contains 25 elements. We have also that $f(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{F}_3$ (we have $f(0) = 2$, $f(1) = 1$, $f(2) = 2$). Then the field $F_3[x]/(x^3+x^2+2)$ contains $3^3 = 27$ elements.

Exercise 10. *(a) Show that the polynomial $X^4 + X + 1$ is irreducible over $\mathbb{F}_2$.*

(b) Let I be the ideal $(X^4 + X + 1)$ in $\mathbb{F}_2[X]$. Find the number of elements in the field $\mathbb{F}_2[X]/I$ and the inverse of the element $g = [X+1]_I$.

(c) List all irreducible polynomials of degree 4 over $\mathbb{F}_2$.

Solution 10. (a) The polynomial $f(X) = X^4 + X + 1$ is irreducible in $\mathbb{F}_2[X]$. We'll prove that $f(X)$ cannot be factor as a product either of a polynomial of degree 1 with a polynomial of degree 3 or of two polynomials of degree 2. Suppose f is the product of two polynomials respectively of degree 3 and 1. Then $f(X)$ would have a root in $\mathbb{F}_2[X]$. But in $\mathbb{F}_2$ one has: $f(0) = 1$ and $f(1) = 1$. Therefore $f(X)$ cannot be factored by polynomials of degree 1 and 3. Now, suppose $f(X)$ is the product of two polynomial of degree 2. The polynomials of degree 2 in $\mathbb{F}_2[X]$ are X^2, $X^2 + X$, $X^2 + 1$, and $X^2 + X + 1$. The first and second of these polynomials are divisible by X, and hence we can return to the previous case. The third polynomial has 1 as a root, and hence we can return to the first case. The last polynomial, $X^2 + X + 1$, is the only irreducible polynomial of degree 2 in $\mathbb{F}_2[X]$. So if $f(X)$ were not irreducible, it would have to be equal to

$$(X^2 + X + 1)^2 = X^4 + 2X^3 + 3X^2 + 2X + 1 = X^4 + X^2 + 1.$$

But it's not, hence $f(X)$ is irreducible in $\mathbb{F}_2[X]$.

(b) Since $f(X) = X^4 + X + 1$ is irreducible in $\mathbb{F}_2[X]$ and $\mathbb{F}_2$ is a field with 2 elements, we know that $\mathbb{F}_2[X]/I$, where $I = (f(X))$, is a field with $2^4 = 16$ elements (since $\deg(f) = 4$). Now, we want to find the inverse of g in the field $\mathbb{F}_2[X]/I$. Meaning that we are looking for a polynomial h such that $gh \equiv 1 \pmod f$, or equivalently $gh + kf = 1$ for some $k \in \mathbb{F}_2[X]$. The Euclidean algorithm can be used to find h and k. Dividing f by g we obtain:

$$f = (X^3 - X^2 + X) \cdot g + 1$$

Thus, we know that $1 = (-X^3 + X^2 - X) \cdot g + f$ and that $[-X^3 + X^2 - X]_I$ is the inverse of g in $\mathbb{F}_2[x]/I$.

(c) Let $Q(X)$ be an irreducible polynomial of degree 4 in $\mathbb{F}_2[X]$. We can write $Q(X)$ in the form $X^4+aX^3+bX^2+cX+d$ with $a, b, c, d \in \mathbb{F}_2$. If $d = 0$, then 0 is a root. Therefore $d = 1$. If exactly one or all three out of a, b, c are zero, then 1 is a root. Therefore either three coefficients a, b, c are nonzero, or exactly two of them are zeros. Therefore the irreducible polynomials are in the following list:

$$X^4 + X + 1, \quad X^4 + X^2 + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1.$$

In part (a) we found that there exists a unique reducible polynomial of degree 4 that has no roots in $\mathbb{F}_2$, it is $X^4 + X^2 + 1$.Then the irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$ are:

$$X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1.$$

Exercise 11. *Let S_{2k} denote the symmetric group of permutation of $2k$ elements.*

(a) Prove that S_{2k} contains an abelian subgroup of order 2^k such that all of its elements except 1 have order 2.

(b) Determine the decomposition of this subgroup as a direct product of cyclic groups with orders given by the elementary divisors.

Solution 11. (a) We can divide the set of $2k$ elements into k pairs, for example $\{(1, k+1), (2, k+2), \dots (k, 2k)\}$. Then the transpositions $t_1 = (1, k+1)$, $t_2 = (2, k+2)$ ... $t_k = (k, 2k)$ are disjoint cycles of order 2, and therefore they pairwise commute: $t_i t_j = t_j t_i$ for any $1 \le i, j \le k$. We also have $t_i^2 = 1$ for all $1 \le i \le k$. Let K be the subgroup of S_{2k} generated by the elements $\{t_1, t_2, \dots t_k\}$. Then it is abelian, and the order of any nontrivial element is 2: indeed $(t_{i_1} t_{i_2} \dots t_{i_r})^2 = t_{i_1}^2 t_{i_2}^2 \dots t_{i_r}^2 = 1$. The order of the group is equal to the sum of the numbers of choices of m elements out of k elements, when m runs from 0 to k (this lists the group elements according to the disjoint transpositions in each element). Then

$$|K| = \sum_{m=0}^{k} \binom{k}{m} = (1+1)^k = 2^k.$$

(b) Since the order of the group K is 2^k, any nontrivial subgroup has the order 2^i for $1 \le i \le k$. Suppose C_{2^i} is present in the decomposition of K into a direct product of cyclic groups according to the classification theorem of finite abelian groups. Then K contains an element of order 2^i. Since all elements of K have order 2, the only possibility is $i = 1$, and therefore K is isomorphic to a direct product of k copies of the group C_2:

$$K \simeq C_2 \times C_2 \times \dots \times C_2 = (C_2)^{\times k}.$$

The elementary divisors of K are $(2, 2, \dots 2)$ (2 is repeated k times).

Exercise 12. *Let S_n denote the symmetric group of permutation of n elements, and suppose that $n \geq k_1 + k_2 + \ldots + k_r$ for some integers $k_i \geq 2$. Let $t \in S_n$ be a product of disjoint cycles of lengths $k_1, k_2, \ldots k_r$,*

$$t = \pi_{k_1} \pi_{k_2} \ldots \pi_{k_r}.$$

Find the order of the element t in S_n.

Solution 12. Suppose that $t^m = 1 \in S_n$ for some $m \in \mathbb{N}$. Then since the disjoint cycles commute, we have

$$t^m = (\pi_{k_1} \pi_{k_2} \ldots \pi_{k_r})^m = \pi_{k_1}^m \pi_{k_2}^m \ldots \pi_{k_r}^m = 1.$$

Disjoint cycles have disjoint orbits of action on the set of n elements. Therefore for the product of disjoint cycles $\pi_{k_i}^m$ to be 1, it is necessary for each disjoint cycle to act trivially on its orbit, meaning that $\pi_{k_i}^m = 1$ for all $1 \leq i \leq r$. The order of a cycle is equal to its length, and therefore $k_i \mid m$ for all $1 \leq i \leq r$. So m is a multiple of each of the k_i. Then by definition the order of t, it should be the least common multiple of the numbers $k_1, k_2, \ldots k_r$, and finally we have that the order of t equal to $\mathrm{lcm}(k_1, k_2, \ldots k_r)$.

Exercise 13. *Let S_5 denote the symmetric group of permutation of 5 elements. Let $a = (135)(24) \in S_5$, and $b = (134)(24) \in S_5$.*

(a) Find the order of a and b in S_5.

(b) Let $A = \langle a \rangle \subset S_5$ and $B = \langle b \rangle \subset S_5$ be the subgroups generated by these elements in S_5. Find the orbit of the element 1 with respect to the action of A and B, and its stabilizer subgroup in A and B, and show how the Orbit-Stabilizer theorem works in these cases.

Solution 13. (a) The element $a = (135)(24)$ is a product of disjoint cycles of lengths 3 and 2, therefore its order is $\mathrm{lcm}(3, 2) = 6$. (See Exercise 12). The element $b = (134)(24)$ is not a product of disjoint cycles. To understand its structure, let us write it in terms of the disjoint cycles. We observe that b sends 1 to 3, then 3 to 4, then 4 to 2, then 2 to 4 which goes further to 1. Therefore $b = (1342)$ and it has order 4.

(b) A is a cyclic group of order 6. The orbit of the element 1 under this group is $\{1, 3, 5\}$ of order 3. The stabilizer subgroup of the element 1 in A is the subgroup generated by the transposition (24) of order 2. The Orbit-Stabilizer theorem holds: $6 = |A| = |\mathrm{Orb}(1)| \cdot |\mathrm{Stab}_1| = 3 \cdot 2$.
The group B is cyclic of order 4. The orbit of 1 under the action of B is the set $\{1, 3, 4, 2\}$ of order 4. The stabilizer subgroup of 1 in B is trivial. The Orbit-Stabilizer theorem holds: $4 = |B| = |\mathrm{Orb}(1)| \cdot |\mathrm{Stab}_1| = 4 \cdot 1$.

Exercise 14. *What is the smallest symmetric group that contains a subgroup isomorphic to*
(a) C_{60},
(b) C_{110},
(c) C_{27} ?

Solution 14. Clearly we have $C_n \subset S_n$ for any n, where the subgroup C_n is generated by an n-cycle. But often we can find a smaller symmetric group containing C_n. Suppose $t \in S_m$ generates a subgroup isomorphic to C_n. Recall that any element of a symmetric group can be written (uniquely up to reordering of cycles) as a product of disjoint cycles. We also know from Exercise 12 that the order of an element is the least common multiple of the lengths of the cycles in its decomposition. So we need to find a set of positive numbers $k_1, k_2, \ldots k_r$ with $\mathrm{lcm}(k_1, k_2, \ldots k_r)$ equal to n and the sum $k_1 + k_2 + \ldots + k_r$ a minimum. Then the product of disjoint cycles of lengths $k_1, k_2, \ldots k_r$ will have the required order and fit into the smallest possible symmetric group.

(a) We have $60 = 2^2 \cdot 3 \cdot 5$, then $\mathrm{lcm}(3, 4, 5) = 60$ and $3 + 4 + 5 = 12$. This provides the minimum of the sum of lengths, because the length of at least one of the cycles has to be divisible by 3, 4, 5. So S_{12} is the smallest symmetric group containing C_{60} as a subgroup, generated by a product of disjoint cycles of lengths $3, 4, 5$.

(b) We have $110 = 2 \cdot 5 \cdot 11$, and by a similar argument we have $\mathrm{lcm}(2, 5, 11) = 110$ and $2 + 5 + 11 = 18$ is the minimum of the sum of lengths. So S_{18} is the smallest symmetric group containing C_{110} as a subgroup, generated by a product of disjoint cycles of lengths $2, 5, 11$.

(c) We have $27 = 3^3$. Here since the order 27 is a power of a prime, it is the least common multiple only of copies of itself. So we must have a cycle of length 27, and S_{27} is the smallest symmetric group containing C_{27} as a subgroup, generated by a cycle of length 27.