## 3.6.11

Is $\mathbb{Z}_4 \oplus \mathbb{Z}_8$ isomorphic to $\mathbb{Z}_{32}$?

## Solution

No, the groups have the same number of elements, but $\mathbb{Z}_{32}$ has an element of order 32, but $\mathbb{Z}_4 \oplus \mathbb{Z}_8$ has no such element. In fact, the element $(a, b) \in \mathbb{Z}_4 \oplus \mathbb{Z}_8$ has order $\mathrm{lcm}(|a|, |a|)$, which it is at most 8.

## 3.6.14

Consider the groups $\mathbb{Z}_{60}$ and $\mathbb{Z}_{30} \oplus \mathbb{Z}_2$. How many elements of orders $2, 3, 4, 5$ does each group have.

## Solution

For $\mathbb{Z}_{60}$, order of an element $[a]$ is $\frac{\mathrm{lcm}(a,60)}{a} = \frac{60}{\gcd(a,60)}$. For $\mathbb{Z}_{30} \oplus \mathbb{Z}_2$ we use the same formula, combined with the fact that $|(a, b)| = \mathrm{lcm}(|a|, |b|)$.

| Elements of order: | $\mathbb{Z}_{60}$ | $\mathbb{Z}_{30} \oplus \mathbb{Z}_2$ |
|---|---|---|
| 2 | 1 | 3 |
| 3 | 2 | 2 |
| 4 | 2 | 0 |
| 5 | 4 | 4 |

## 4.5.11

Show that $D_3$ is isomorphic to the affine group $\mathrm{Aff}(3)$ of matrices $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ with $a, b \in \mathbb{Z}_3$ and $a \neq 0$. The group operation is matrix multiplication.

## Solution

Let $D_3$ be the group generated by $R, F$ with relations $R^3 = F^2 = I$ and $RF = FR^2$. Also note that $\mathrm{Aff}(3)$ has exactly 6 elements, the same number as $D_3$. We define the matrices:

$$M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad N = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

A straightforward computation shows that $M, N$ satisfy the same relations as $R, F$. Furthermore, the same computations show that $M, N$ generate a group of 6 elements, which must therefore be all of $\mathrm{Aff}(3)$. Therefore, we define a map $F\colon \mathrm{Aff}(3) \to D_3$ by $M \mapsto R$ and $N \mapsto F$. It is well defined since $M, N$ satisfy the same relations as $R, F$. Since the image of $F$ contains generators of $D_3$ $F$ must be surjective. Since the domain and target of $F$ have the same (finite) number of elements, $F$ must then also be injective, so it is a bijection.

## 4.5.13

Consider the affine group $\mathrm{Aff}(4)$ of matrices $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ with $b \in \mathbb{Z}_4$ and $a \in \mathbb{Z}_4^*$, with group operation given by matrix multiplication. Which of the groups of order 8 is $\mathrm{Aff}(4)$ isomorphic to?

## Solution

The groups of order 8 are:

1. $Z_8$
2. $Z_2 \oplus \mathbb{Z}_4$
3. $Z_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
4. $D_4$
5. $Q$

The group Aff(4) is non-abelian since

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

which leaves $D_4$ and $Q$ as the remaining possibilities. It is easy to see that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ generates an order 4 subgroup, and that

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

characterizing Aff(4) as the group $D_4$ by Case 1 on p.147. For an explicit isomorphism, one can take

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto F$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \mapsto R$$

## 5.4.11

Find all maximal ideals in $\mathbb{Z}_{18}$.

## Solution

One way of solving this is following the idea from Example 2 on the previous page. Here is a different approach, based on the Chinese Remainder Theorem. By the CRT we know that $\mathbb{Z}_{18}$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_9$. From exercise 5.4.21 we know that the ideals in $\mathbb{Z}_2 \oplus \mathbb{Z}_9$ are of the form $I_1 \oplus I_2$, where $I_1 \subset \mathbb{Z}_2$ and $I_2 \subset \mathbb{Z}_9$ are ideals. Assume $I_1$ and $I_2$ are proper ideals in their respective rings, then $I_1 \oplus I_2 \subset I_1 \oplus \mathbb{Z}_9$ and $I_1 \oplus I_2 \subset \mathbb{Z}_2 \oplus I_2$, which are all proper ideals. So the maximal ideals of $\mathbb{Z}_2 \oplus \mathbb{Z}_9$ must be of the form $I_1 \oplus \mathbb{Z}_9$ and $\mathbb{Z}_2 \oplus I_2$ for maximal ideals $I_1 \subset \mathbb{Z}_2$ and $I_2 \subset \mathbb{Z}_9$. $\mathbb{Z}_2$ is a field, so its only maximal ideal is $(0)$. In $\mathbb{Z}_9$, the only non-units are multiples of 3, which form the unique maximal ideal. Therefore, $\mathbb{Z}_2 \oplus \mathbb{Z}_9$ has two maximal ideals $(0) \oplus \mathbb{Z}_9$ and $\mathbb{Z}_2 \oplus (3)$, which are generated by $(0, 1)$ and $(1, 3)$ respectively. Taking the inverse image by the CRT isomorphism shows that the two maximal ideals of $\mathbb{Z}_{18}$ are generated by $(10)$ and $(3)$

## 5.4.19

Suppose that $R, S, T, V$ are rings such that $R \simeq T, S \simeq V$. Show that $R \oplus S \simeq T \oplus V$.

## Solution

Let $f\colon R \to T$ and $g\colon S \to V$ be isomorphisms. Consider $h\colon R \oplus S \to T \oplus V$ defined by $h((a,b)) = (f(a), g(b))$. We wish to show that $h$ is an isomorphism. It straightforward to check that it is a ring homomorphism, so we must check that it is a bijection. For injectivity, assume that $h((a,b)) = (0,0)$. Then, from the definition of $h$ we see that $f(a) = 0$ and $g(b) = 0$. Since $f$ and $g$ are isomorphisms and therefore injective we must have $a = 0$ and $b = 0$, so $(a,b) = (0,0)$. To check surjectivity let $(t,v) \in T \oplus V$, since $f, g$ are surjective pick $r \in R, s \in S$ such that $f(r) = t$ and $g(s) = v$, then $h((r,s)) = (t,v)$, so $h$ is surjective.

## 5.4.21

See previous weeks solutions

## 6.2.11

Suppose you have some beads in a jar and you know that when you take them out three at a time you have two left, but when you take them out five at a time you have four left, and finally when you take them out seven at a time you have six left. How many beads are in the jar?

## Solution

The CRT gives an isomorphism $\mathbb{Z}_{105} \to \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$ given by $[a]_{\mathbb{Z}_{105}} \mapsto ([a]_{\mathbb{Z}_3}, [a]_{\mathbb{Z}_5}, [a]_{\mathbb{Z}_7})$ and we wish to find the inverse image of $(2,4,6)$ under this isomorphism. The simplest way of doing this is to note that the inverse of $(2,4,6)$ is $(1,1,1)$, and the inverse image of $(1,1,1)$ is 1. It follows that the inverse image of $(2,4,6)$ is the inverse of 1, which is 104. We can conclude that the smallest possible number of beads in the jar is 104.

## 6.2.12

Suppose that $F$ is a field and $f, g \in F[x]$ with $\gcd(f,g) = 1$. Show that $F[x]/(fg) \simeq F[x]/(f) \oplus F[x]/(g)$.

## Solution

This is the analogue of the CRT for polynomial rings. To solve the exercise we follow a similar idea to the proof of the CRT. Let $T\colon F[x] \to F[x]/(f) \oplus F[x]/(g)$ be defined by $h \mapsto (h(\mod f), h(\mod g))$, and we wish to study the kernel and image of $T$. Assume $p \in \ker T$. Then $p = af = bg$ for some $a, b \in F[x]$. Since $\gcd(f,g) = 1$, $g$ must divide $a$, so $p$ divides $fg$. This means that $p \in (fg)$. Thus $\ker T \subseteq (fg)$. Since the reverse inclusion clearly holds we must have equality.

To prove surjectivity, we know that since $\gcd(f,g) = 1$, there exists $a, b \in F[x]$ such that $af + bg = 1$. From this it follows that $T(af) = (0, [af]) = (0, [af + bg]) = (0, [1])$ and similarily $T(bg) = (1, 0)$. Together with $T(x) = ([x], [x])$, these three elements generate $F[x]/(f) \oplus F[x]/(g)$, so $T$ is surjective. We can now conclude using the first ring isomorphism theorem.

## Exam 2017 Problem 4

a) Let $F$ be a field and assume that $f(x) \in F[x]$ is an irreducible polynomial of degree $n$. Let $K$ be a splitting field for $f(x)$. Explain why $n \leq [K : F] \leq n!$. If $N$ is odd and there exists and there exists $\delta \in K$ with $\delta^2 \in F$ but $\delta \notin F$, show that $2n \leq [K : F]$.

b) Assume now that $f$ is an irreducible degree 3 polyonmial in $\mathbb{Q}[x]$ and let $K$ be a splitting field for $f$. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f$ in $K$. Let $S_3$ be the permutation group on these roots and let $G$ the Galois group. Define $\delta = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \in K$ and set $D = \delta^2$. Show that if $\sigma \in G$ then $\sigma(D) = D$. Explain why this implies that $D \in \mathbb{Q}$. Prove that $D$ is not a square in $\mathbb{Q}$, then $[K : \mathbb{Q}] = 6$ and $G \simeq S$.

c) Let $\tau$ be a transposition in $S$. Prove that $D$ is a square in $\mathbb{Q}$ then $\tau \notin G$ (Hint: What does $\tau$ do to $\delta$?) Use this to show that $D$ is a square in $\mathbb{Q}$ then $[K : \mathbb{Q}] = 3$ and $G \simeq \mathbb{Z}_3$.

## Solution

a) We prove this by induction. If $f$ has degree 1 the result is obvious. Let $\alpha$ be a root of $f$. Since $f$ is irreducible, it is the minimal polynomial of $\alpha$, so the extension $F(\alpha)$ has degree $n$. Since $F(\alpha)$ is a subfield of $K$, $K$ must be an extension of degree at least $n$. In $F(\alpha)$ $f$ has at least one root, so it factors as $f = (x - \alpha)h$, where $h$ has degree $n - 1$. By induction, the splitting field $K$ of $h$ over $F(\alpha)$ has degree at most $(n - 1)!$. Therefore the extension $[F(\alpha) : F][K : F(\alpha)]]$ has degree at most $n(n - 1)! = n!$.

To see the second statement, let $g$ be the minimal polynomial of $\delta$, which will have degree 2, since $\delta^2 \in F$. Observe also that since $K$ is a field extension of $F(\alpha)$ $n$ must divide $[F : K]$. So it suffices to check that $g$ does not split over $F(\alpha)$. But if $g$ splits in $F(\alpha)$, then $F(\delta)$ is a subfield of $F(\alpha)$, so $[F(\delta) : F][F(\alpha) : F(\delta)] = [F(\alpha) : F]$. But the left hand side is even, and the right hand side is odd, a contradiction.

b) We know that $\sigma \in G$ permutes the roots $\alpha_i$. But $D = \delta^2$ is invariant under these permutations. Therefore, $D$ is in the fixed field of all $\sigma \in G$, which only holds for $D \in \mathbb{Q}$. If $D$ is not a square in $\mathbb{Q}$ then $[K : \mathbb{Q}]$ we get $2 \cdot 3 \leq [K : \mathbb{Q}] \leq 3!$ by the previous part, proving that $[K : \mathbb{Q}] = 6$. Thus, $G$ is an order 6 subgroup of $S$, hence $G \simeq S$.

c) Any transposition of the $\alpha_i$ will switch the sign of $\delta$, but keep $D$ fixed. If $D$ is a square in $\mathbb{Q}$, then the square root must be $\delta \in \mathbb{Q}$. But then the transposition acts non-trivially on $\delta \in \mathbb{Q}$, proving that $\tau \notin G$. So if $D$ is a square in $\mathbb{Q}$, $G$ contains no transpositions. But since $G$ is a subgroup of $S_3$, the only subgroup with no transpositions is $\mathbb{Z}_3$.

## Exam 2006 Problem 1

a) Explain why the automorphism group of the additive group $\mathbb{Z}_n$ is isomorphic to the multiplicative group $\mathbb{Z}_n^*$ of units of the ring $\mathbb{Z}_n$.

b) Show that if $p \neq 2$ is prime then $\mathbb{Z}_p^*$ has only one element of order 2. Conclude that $a \mapsto -a$ is the only automorphism of order 2 of the additive group $\mathbb{Z}_p$.

c) Let $P$ be a prime, $p \neq 2$, and $K$ a group of order $2p$. What can you say about the number of Sylow 2-subgroup and $p$-subgroup of $K$ using Sylow's theorems

## Solution

1. $\mathbb{Z}_n$ is a cyclic group, so an group homomorphism is determined by the value on the generator 1. For the homomorphism to be surjective, the image must be a generator of $\mathbb{Z}_n$, so an automorphism of $\mathbb{Z}_n$ maps 1 to an element of $\mathbb{Z}_n^*$, which determines the automorphism completely. It is also straightforward to check that if automorphisms $F, G$ of $\mathbb{Z}_n$ maps 1 to $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n^*$ respectively, the composition $F \circ G$ maps 1 to $ab$.

2. We know that if $p$ is prime $\mathbb{Z}_p^*$ is a cyclic group. If $p$ is odd, the cyclic group $\mathbb{Z}_p^*$ has even order. A cyclic group of even order has a single element of order 2. Therefore, there is a single automorphism of $\mathbb{Z}_p$ which has order 2. The map $a \mapsto -a$ has order 2, so it must be the unique one.

3. Let $n_2$ and $n_p$ be the number of Sylow 2- and $p$-subgroups respectively. By the third Sylow theorem, $n_2$ divides $p$ and $n_2 \cong 1 \mod 2$, which gives two possibilities $n_2 = 1$ or $n_2 = p$ since $p$ is a prime. On the other hand, $n_p$ divides 2, so $n_p = 1$ or $n_p = 2$. Also $n_p \cong 1 \mod p$, but this is cannot happen if $n_p = 2$. Therefore we must have $n_p = 1$.

## Additional exercise

Describe the value of the Frobenius $\sigma_3$ on every element of the field $F_9$ from the example in section 6.3. Find the fixed field of $\sigma_3$.

## Solution:

We recall that $\sigma_3(x) = x^3$. We think of the field $F_9$ as $\mathbb{F}_3[x]/(x^2+1)$ We can set up the follow table:

| $x$ | $\sigma(x)$ |
|---|---|
| $0$ | $0$ |
| $1$ | $1$ |
| $2$ | $2$ |
| $x$ | $2x$ |
| $2x$ | $x$ |
| $x+1$ | $2x+1$ |
| $x+2$ | $2x+2$ |
| $2x+1$ | $x+1$ |
| $2x+2$ | $x+2$ |