

Partial Solutions to Homework 8

1. Stewart, part (c) for each of the exercises 12.1, 12.2, 12.3, 12.4, 12.5, 12.6.

Hint: First compute the complex zeros, and show that there exist zeros α_1, α_2 such that $\alpha_2 = \frac{2}{\alpha_1}$.

Solution:

The polynomial $t^4 - 3t^2 + 4$ is irreducible and has four roots $\pm\alpha, \pm\frac{2}{\alpha}$, where $\alpha = \sqrt{\frac{3+i\sqrt{7}}{2}}$. So the splitting field is $\mathbb{Q}(\alpha)$, of degree 4 over \mathbb{Q} . The Galois group has four elements, and since all roots have the same minimal polynomial, the four elements of the Galois group have the property $\gamma_1 = id$ s.t. $\gamma_1(\alpha) = \alpha, \gamma_2(\alpha) = -\alpha, \gamma_3(\alpha) = \frac{2}{\alpha}, \gamma_4(\alpha) = -\frac{2}{\alpha}$. The values on α also determine the values on the other zeros of the polynomial, and one obtains a group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. The Galois group Γ has the subgroups $\{id\}, \Gamma$, and $\{id, \gamma_2\}, \{id, \gamma_3\}, \{id, \gamma_4\}$, all of which are normal since Γ is abelian. The corresponding fixed fields are $\mathbb{Q}(\alpha), \mathbb{Q}, \mathbb{Q}(\alpha^2) = \mathbb{Q}(\frac{3+i\sqrt{7}}{2}) = \mathbb{Q}(i\sqrt{7}), \mathbb{Q}(\alpha + \frac{2}{\alpha}) = \mathbb{Q}(\sqrt{7}),$ and $\mathbb{Q}(\alpha - \frac{2}{\alpha}) = \mathbb{Q}(i)$. They are splitting fields for the polynomials $t^4 - 3t^2 + 4, 1, t^2 + 7, t^2 - 7, t^2 + 1$ respectively, so all of them are normal. The Galois groups of $\mathbb{Q}(\alpha), \mathbb{Q}$ are clear, the Galois groups of the respective quadratic fields over \mathbb{Q} are isomorphic to \mathbb{Z}_2 , for example again by the fundamental theorem. But these groups are exactly the respective quotient groups of Γ .

2. Find presentations for the groups $\mathbb{Z}_4 \times \mathbb{Z}_8, D_{10}$ and \mathbb{Q} .

Solution:

One possibility:

$$\mathbb{Z}_4 \times \mathbb{Z}_8 \cong \langle a, b : a^4 = b^8 = 1, ab = ba \rangle.$$

$$D_{10} \cong \langle \sigma, \tau : \sigma^5 = \tau^2 = 1, \tau\sigma = \sigma^4\tau \rangle.$$

$\mathbb{Q} \cong \langle a_i (i = 1, 2, 3, \dots) : a_i^k a_j^l = a_{ij}^{il+jk}, a_{ij}^i = a_j (i, j = 1, 2, 3, \dots \text{ and } k, l \in \mathbb{Z}) \rangle$ (here a_j stands for the fraction $\frac{1}{j}$, and the relations encode the addition and canceling the common factors of numerator and denominator).

3. Let $m \geq 2, n \geq 2$ be positive integers. We want to construct groups of order mn . Let a, b be two “letters” and $G = \{a^i b^j \mid 0 \leq i < m, 0 \leq j < n\}$ be the set with mn elements which are the “words” $a^i b^j$. Let r be an integer such that $0 \leq r < m$.

Define multiplication on G by $a^s b^t \cdot a^u b^v = a^x b^y$, where x is the remainder of $s + u \cdot r^t$ when divided by m , and y is the remainder of $t + v$ when divided by n .

(The idea is the following: we want that a has order m , b has order n , and that the subgroup generated by a is normal. Then bab^{-1} is contained in the subgroup generated by a , and it must be equal to a^r for some r . So we must have $bab^{-1} = a^r$ which is equivalent to $ba = a^r b$. But then $b^t a^u = a^{ur^t} b^t$ and the definition must be as it is.)

a) Show that this defines a group structure on G if and only if $r^n \equiv 1 \pmod{m}$.

Suggestion: Show that if $r^n \equiv 1 \pmod{m}$, it makes sense to interpret exponents of powers of a modulo m and exponents of powers of b modulo n , and one has $a^s b^t \cdot a^u b^v = a^{s+ur^t} b^{t+v}$ for all $s, t, u, v \in \mathbb{Z}$. Deduce associativity from this. In the other case show that $b(b^{n-1}a) \neq (b \cdot b^{n-1})a$.

b) Show that the presentation $\langle a, b \mid a^m = b^n = 1, ba = a^r b \rangle$ defines a group of order mn if and only if $r^n \equiv 1 \pmod{m}$.

- c) We'll see as an example in the lecture that every group of order 15 has a unique subgroup of order 5 which is normal, and that every group of order 15 has a subgroup of order 3. Use this statement and the preceding part to prove that every group of order 15 is abelian.

Solution:

a) If $r^n \not\equiv 1 \pmod{m}$, then $a^0 b^1 (a^0 b^{n-1} \cdot a^1 b^0) \neq (a^0 b^1 \cdot a^0 b^{n-1}) \cdot a^1 b^0$, so we cannot have a group structure. If $r^n \equiv 1 \pmod{m}$, then the multiplication rule shows that $1 = a^0 b^0$ is identity, $a^{m-1} = a^{m-1} b^0$ is an inverse for a , and $b^{n-1} = a^0 b^{n-1}$ is an inverse for b . So we should consider exponents of powers of a modulo m and exponents of powers of b modulo n , and this behaves well with respect to the multiplication rule: if we change, in the factors, exponents of powers of a by a multiple of m and exponents of powers of b by a multiple of n , then in the product, the exponents also change by such multiples. It follows that one has $a^s b^t \cdot a^u b^v = a^{s+ur^t} b^{t+v}$ for all $s, t, u, v \in \mathbb{Z}$. But then associativity follows from a simple computation. The inverse to $a^u b^v$ is $b^{-v} a^{-u}$. So we get a group structure.

b) The group presentation shows that every element of the group can be written as $a^i b^j$, where $| 0 \leq i < m, 0 \leq j < n$. (Use the third relation to move all a 's in front of all b 's.) Now suppose all of these mn elements are distinct, then we must be in the situation of the preceding part, so we must have $r^n \equiv 1 \pmod{m}$. On the other hand, if $r^n \equiv 1 \pmod{m}$, we see that there is a surjective homomorphism from the group defined by the presentation to the group G from the preceding part. So the group defined by the presentation must have at least mn different elements.

c) Let G be a group of order 15, and let $a \in G$ be a generator of the unique subgroup of order 5, and let $b \in G$ have order 3. Then all elements $a^i b^j$ where $| 0 \leq i < 5, 0 \leq j < 3$ are distinct, so these are the 15 elements of the group. Since a generates a normal subgroup, we must have $bab^{-1} = a^r$ for some r such that $0 \leq r < 5$. By the first part, we must have $r^3 \equiv 1 \pmod{5}$. But this implies that $r = 1$, so we have $ba = ab$ and the group G is abelian and cyclic, by the structure theorem of finitely generated abelian groups.

4. Free objects in other categories.

- a) Let G be an abelian group. We write the group addition additively as $a + b$. As usual, we use the abbreviation (for $n \in \mathbb{Z}, a \in A$) for a sum with $|n|$ terms:

$$n \cdot a = \begin{cases} a + a + \dots + a & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ (-a) + (-a) + \dots + (-a) & \text{if } n < 0. \end{cases}$$

Now G is by definition a **free abelian group** if G has a **basis**, i.e. a subset $B = \{b_i\} \subseteq G$ such that each element $g \in G$ is a unique linear combination with integral coefficients of finitely many of the b_i : there are unique $\lambda_i \in \mathbb{Z}$, all but finitely many of them zero, such that $g = \sum \lambda_i b_i$.

Remark: Similarly to the case of free groups, one can also define the free abelian group generated by a set A : it consists of all formal linear combinations $\sum \lambda_i a_i$ of finitely many elements $a_i \in A$ with integer coefficients λ_i , and has A as a basis.

Let G be a free abelian group with basis $B = \{b_i \mid i \in I\}$, let G' be an abelian group, and let $a_i \in G'$ for $i \in I$. Prove that there exists a unique group homomorphism $\phi : G \rightarrow G'$ such that $\phi(b_i) = a_i$.

- b) Let K be a field. A commutative K -algebra is a commutative ring A with unit, which contains K as a subring. A homomorphism of commutative K -algebras $f : A \rightarrow B$ is a ring homomorphism such that $f(x) = x$ for all $x \in K$.

A **free commutative K -algebra** is a commutative K -algebra A with a subset $T = \{t_i \mid i \in I\} \subseteq A$ such that for all commutative K -algebras B and elements $b_i \in B$ for $i \in I$ there exists a unique homomorphism of commutative K -algebras $\phi : A \rightarrow B$ such that $\phi(t_i) = b_i$. Find some free commutative K -algebras (you know some examples!).

Remark: Similarly to the case of free groups, one can also define the free commutative K -algebra generated by a set T . In fact we have done this for finite sets T (but we have called it differently...), and a similar definition also works for infinite sets T .

- c) Let K be a field. Recall (I hope you have seen this in your linear algebra class) that every K -vector space V has a basis, i.e. a subset $B = \{b_i\} \subseteq V$ such that each element $v \in V$ is a unique linear combination with coefficients in K of finitely many of the b_i .

Prove (using this statement) that every K -vector space V is free: i.e. prove that if $B = \{b_i\} \subseteq V$ is a basis, W is a K -vector space, $w_i \in W$ for $i \in I$ then there exists a unique vector space homomorphism (K -linear map) $\phi : V \rightarrow W$ such that $\phi(b_i) = w_i$.

Summary: In all cases, given a set A , and an object B (a group/abelian group/commutative K -algebra/ K -vector space/...) the set of homomorphisms (of groups/...) from the free object $F[A]$ generated by A and the object B is in bijection with the set of maps of sets from A to the underlying set $U(B)$ of (the group/...) B :

$$\text{Hom}(F[A], B) \cong \text{Maps}_{\text{Sets}}(A, U(B)).$$

Solution:

a) If $\phi : G \rightarrow G'$ is a group homomorphism such that $\phi(b_i) = a_i$, then we must have (using the homomorphism property) that $\phi(\sum \lambda_i b_i) = \sum \lambda_i a_i$. On the other hand, this formula defines indeed a group homomorphism from G to G' (check that the value on a sum of two linear combinations is the sum of the values on each of the linear combinations). So there is exactly one such homomorphism.

b) All polynomial rings over K are free commutative K -algebras: Consider $K[t_1, \dots, t_n]$, with $T = \{t_i\}$. Then for any commutative K -algebra B and elements $b_i \in B$, we have a unique homomorphism of commutative K -algebras $\phi : K[t_1, \dots, t_n] \rightarrow B$ such that $\phi(t_i) = b_i$: ϕ must map $\sum_J a_J t_1^{j_1} \dots t_n^{j_n}$ to $\sum_J a_J b_1^{j_1} \dots b_n^{j_n}$, and this defines indeed a ring homomorphism which is the identity on K . (Check that sums map to sums and products map to products.)

It also makes sense to define polynomial rings in infinitely many indeterminates, i.e. for each set T of indeterminates. Elements are sums of finitely many monomials, and in each of the monomials only finitely many indeterminates occur. c) Again $\phi : V \rightarrow W$ has to be defined by $\phi(\sum \lambda_i b_i) = \sum \lambda_i w_i$, and this is a K -linear map.