Final exam MAT2410, autumn 2022, solutions

May 22, 2023

1. (a) Prove that the set
$$S = \{2^n \mid n \in \mathbb{Z}\},$$
equipped with the usual operation of multiplication, is a group.

   (b) List all finite abelian groups of order 20, up to isomorphism.

   (c) Let A_4 be the alternating group on 4 letters, that is the subgroup of S_4 consisting of even permutations. Find elements $\sigma_1, \sigma_2, \sigma_3 \in A_4$ such that σ_1 has order 1, σ_2 has order 2, and σ_3 has order 3.

   (d) Prove that A_4 is not abelian.

Solution:

(a) The binary operation of multiplication is associative. The element $1 = 2^0 \in S$ is an identity element for the operation of multiplication. For every $n \in \mathbb{Z}$, we have an inverse to $2^n \in S$ given by $2^{-n} \in S$. Hence S is a group.

Alternatively: We know that the non-zero rational numbers $\mathbb{Q}^*$ with the operation of multiplication forms a group. We then have S is the cyclic subgroup of $\mathbb{Q}^*$ generated by $2 \in \mathbb{Q}^*$.

(b) By the fundamental theorem of finitely generated abelian groups, we know that if G is an abelian group of order 20, we can write
$$G \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}},$$
where the p_i are primes, the e_i are positive integers, where $\prod_{i=1}^n p_i^{e_i} = 20$, and where this presentation is unique up to reordering the factors. We can express 20 as a product of prime powers in two ways: $20 = 2^2 \times 5$ and $20 = 2 \times 2 \times 5$, and this gives us two abelian groups or order 20:
$$\mathbb{Z}_4 \times \mathbb{Z}_5$$
and
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5.$$

(c) Let $\sigma_1 = e$, the identity element in A_4. Since $e^1 = e$, we have that e has order 1.

Let $\sigma_2 = (1,2)(3,4)$. Since σ_2 is the product of two transpositions, it is even, hence $\sigma_2 \in A_4$. We have $\sigma_2^2 = e$, and so the order of σ_2 is 2.

Let $\sigma_3 = (1,2,3) = (1,2)(2,3)$. Again since σ_3 is the product of two transpositions, it is an even permutation, so $\sigma_3 \in A_4$. We have $\sigma_3^2 = (1,3,2)$ and $\sigma_3^3 = e$, so the order of σ_3 is 3.

(d) With σ_2, σ_3 as above, we compute that

$$\sigma_2\sigma_3 = (1,2)(3,4)(1,2,3) = (2,4,3),$$

while

$$\sigma_3\sigma_2 = (1,2,3)(1,2)(3,4) = (3,4,1).$$

Since $\sigma_2\sigma_3 \neq \sigma_3\sigma_2$, we see that A_4 is not abelian.

2. (a) Determine the 0-divisors in the ring $\mathbb{Z}_{10}$.

(b) Let R be the ring $\mathbb{Z} \times \mathbb{Z}$, where addition and multiplication is given by, for $(a,b),(c,d) \in R$, setting

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b)(c,d) = (ac, bd).$$

Let

$$I = \{(a,0) \mid a \in \mathbb{Z}\} \subset R$$

Prove that I is an ideal of R.

(c) Prove that I above is a prime ideal, and that I is not a maximal ideal.

Solution:

(a) The 0-divisors of $\mathbb{Z}_{10}$ are the elements $a \neq 0$ such that there is an element $b \neq 0$ with $ab = 0$. The elements $2, 4, 5, 6, 8$ are 0-divisors, since $(2)(5) = (4)(5) = (5)(2) = (6)(2) = (8)(2) = 0$ in $\mathbb{Z}_{10}$. The elements $1, 3, 7, 9$ are units and so are not 0-divisors, since $(1)(1) = (3)(7) = (7)(3) = (9)(9) = 1$.

Alternatively it is known that the zero-divisors in $\mathbb{Z}_n$ are the $1 \leq d \leq n-1$ such that $\gcd(d,n) \neq 1$, which for $n = 10$ gives the list above.

(b) The set I contains $(0,0)$, is closed under addition, and for $(a,0) \in I$ we have $-(a,0) = (-a,0) \in I$. Thus I is a subgroup of $(R,+)$. If $(b,c) \in R$ and $(a,0) \in I$, we have

$$(b,c)(a,0) = (ba,0) = (ab,0) = (a,0)(b,c),$$

and so $(b,c)(a,0), (a,0)(b,c) \in I$. This means that I is an ideal of R.

Alternatively the homomorphism $\pi\colon R \to \mathbb{Z}$ given by $\pi(a,b) = b$ has $\ker\pi = I$, so I is an ideal.

(c) If $(a,b),(c,d) \in R \setminus I$, we have $b \neq 0 \neq d$. Then $(a,b)(c,d) = (ac,bd)$ with $bd \neq 0$, so $(a,b)(c,d) \notin I$. This means that I is a prime ideal.

To show that I is not maximal, consider the set $J = \{(a,2b) \mid a,b \in \mathbb{Z}\} \subset R$. Here J is an ideal strictly containing I with $J \neq R$, so that I is not maximal.

Alternatively Since $\pi\colon R \to \mathbb{Z}$ has $I = \ker \pi$, we have that $R/I \simeq \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, I is prime. Since $\mathbb{Z}$ is not a field, I is not maximal.

3. (a) Let p be a prime number, and let $f(x) = x^p - x \in \mathbb{Z}_p[x]$. What are the zeros of $f(x)$ in $\mathbb{Z}_p$?

   (b) Prove that the ring $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field, and determine its number of elements.

Solution:

(a) Fermat's theorem says that for every $\alpha \in \mathbb{Z}_p$, we have $\alpha^p = \alpha$, and so $\alpha^p - \alpha = 0$. This means that every $\alpha \in \mathbb{Z}_p$ is a zero of $f(x)$.

(b) The polynomial $x^2 + 1 \in \mathbb{Z}_3[x]$ is irreducible, since it is of degree 2 and has no zeros in $\mathbb{Z}_3$, which we can check by evaluating in $0, 1$ and 2:

$$0^2 + 1 = 1, 1^2 + 1 = 2, 2^2 + 1 = 1.$$

It follows that $\langle x^2+1\rangle$ is a maximal ideal of $\mathbb{Z}_3[x]$, and so $F = \mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field. Letting $\alpha = x + \langle x^2+1\rangle$, we have $F = \mathbb{Z}_3(\alpha)$, and so

$$[F : \mathbb{Z}_3(\alpha)] = \deg(\mathrm{irr}(\alpha, \mathbb{Z}_3)) = \deg(x^2+1) = 2.$$

It then follows that $|F| = 3^2 = 9$.

Alternatively every coset of $\langle x^2+1\rangle$ contains a unique element of the form $a + bx$, with $a, b \in \mathbb{Z}_3$. Hence the elements of F are of the form

$$(a + bx) + \langle x^2 + 1\rangle$$

which means there are $3 \times 3 = 9$ elements.

4. Let $f(x) = x^5 - 8x^4 + 2x + 2 \in \mathbb{Q}[x]$. You may use without proof that this polynomial is irreducible.

   (a) Let $\alpha \in \overline{\mathbb{Q}}$ be a zero of $f(x)$. Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, and give a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$.

   (b) Let $\beta \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}$. Prove that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

   (c) Let $E \leq \overline{\mathbb{Q}}$ be the splitting field of $f(x)$ over $\mathbb{Q}$. It can be shown that $G(E/\mathbb{Q}) \simeq S_5$. Using this, show that there exists a field K with $\mathbb{Q} \leq K \leq E$ such that $[K : \mathbb{Q}] = 24$.

Solution:

(a) Since $f(x)$ is irreducible and monic, we have that $\text{irr}(\alpha, \mathbb{Q}) = f(x)$. It follows that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\text{irr}(\alpha, \mathbb{Q})) = 5.$$

A basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space is given by

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4.$$

(b) Since $\beta \neq \mathbb{Q}$, we have that $\mathbb{Q} \neq \mathbb{Q}(\beta)$. The tower of fields $\mathbb{Q} < \mathbb{Q}(\beta) \leq \mathbb{Q}(\alpha)$ gives

$$5 = [\mathbb{Q}(\alpha : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}].$$

Since 5 is a prime and $[\mathbb{Q}(\beta) : \mathbb{Q}] \neq 1$, we must have

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 1, [\mathbb{Q}(\beta) : \mathbb{Q}] = 5.$$

This means that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

(c) The group S_5 has a subgroup $\langle (1, 2, 3, 4, 5) \rangle$ of order 5. Let $H < G(E/\mathbb{Q})$ be a corresponding subgroup of $G(E/\mathbb{Q})$ with $|H| = 5$. Let $K = E_H$. Then

$$[E : K] = |H| = 5,$$

so

$$[K : \mathbb{Q}] = \frac{[E : \mathbb{Q}]}{[E : K]} = \frac{|G(E/\mathbb{Q})|}{5} = \frac{|S_5|}{5} = \frac{120}{5} = 24.$$