EC HW - MATH403

Danesh Sivakumar

May 12th, 2022

The first six problems (7 points each) may be true or false. Give a brief reason why.

1. If K is a field and $L \subseteq K$ is a subring, then L is an integral domain.
   Solution: True; we will show that L has no zero divisors. Suppose $x, y \in L$ with $xy = 0$. Then it follows that $x, y \in K$, meaning that $x = 0$ or $y = 0$ because K is a field.

2. If $\sigma = (123)(45) \in S_5$ and $\tau = (1,2)(3,4,5) \in S_5$ then there exists $\lambda \in S_5$ with $\lambda\sigma\lambda^{-1} = \tau$
   Solution: True; both σ and τ have the same cycle structure (they are each the product of a 2-cycle and 3-cycle), so they are conjugate.

3. There exists a finite field with 24 elements.
   Solution: False; the order of any finite field must always be the power of a prime p, and 24 is not a power of a prime.

4. Every group of order 7 is isomorphic to the multiplicative subgroup of the group of nonzero elements of a finite field.
   Solution: True; every group of order 7 is the same up to isomorphism because 7 is prime, so take any finite field with 7 elements (which is guaranteed to exist because 7 is prime).

5. If G is a group of order 245, then G contains a normal subgroup isomorphic to $\mathbb{Z}_5$
   Solution: True; observe that $245 = 7^2 \cdot 5$, meaning that the number of 5-Sylow subgroups of G is equal to $1 \mod 5$ and divides 49; this implies that there is only one 5-Sylow subgroup, so it is normal due to its uniqeueness. Furthermore, this subgroup has prime order 5, meaning that it must be cyclic and thus isomorphic to $\mathbb{Z}_5$.

6. If H is a subgroup of G with $|G| = 180$ and the index of H in G is 12, then H contains an element of order 3 but no element of order 2.
   Solution: True; observe that $|H| = 180/12 = 15$, and 2 does not divide 15 so there cannot be an element of order 2. However, 3 (a prime) divides 15, and by Cauchy's theorem it follows that there is an element of order 3.

7. Up to isomorphism, there exist exactly two non-isomorphic abelian groups of order 20 called A and B. Which of the following abelian groups of order 20 are isomorphic to A and which are isomorphic to B? a) $\mathbb{Z}_{20}$; b) $\mathbb{Z}_{10} \times \mathbb{Z}_2$; c) $\mathbb{Z}_5 \times \mathbb{Z}_4$; d) U_{25} the units in the ring $\mathbb{Z}_{25}$; e) the subgroup of S_9 generated by $a = (12345)$, $b = (67)$ and $c = (89)$; f) the kernel of the homomorphism $f\colon \mathbb{Z}_{20} \times \mathbb{Z}_2 \to \mathbb{Z}_2$ given by $f(a \mod (20), b \mod (2)) = (a+b) \mod (2)$.
Solution: Suppose A is cyclic and B is not cyclic. Then A is isomorphic to a) [by definition], c) [because 4 and 5 are relatively prime], and d) [because 25 is the power of an odd prime]. Next, B is isomorphic to b) [because 10 and 2 are not relatively prime], e) [because this subgroup is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, which is not cyclic] and f) [because the kernel is all tuples (x, y) such that x and y have the same parity in their respective groups, which is isomorphic to $\mathbb{Z}_{10} \times \mathbb{Z}_2$].

8. Let $f = x^3 + x + 1 \in \mathbb{Z}_3[x]$.

   (1) Determine the unique factorization of f in $\mathbb{Z}_3[x]$.
   (2) Show $\mathbb{Z}_3[x]/(f)$ is isomorphic as rings to the product $\mathbb{Z}_3 \times F$ where F is a field of 9 elements.

   Solution:

   (1) Observe that 1 is a root of f, meaning that $(x-1)$ is a factor. We know that the final answer will have the form $(x-1)(ax^2+bx+c)$; expanding and matching coefficients yields $(x-1)(x^2+x-1)$.
   (2) Observe that $(x-1)$ and (x^2+x-1) are irreducible polynomials in $\mathbb{Z}_3[x]$, meaning that the ideals generated by them are comaximal. Thus, by the Chinese Remainder Theorem there exists an isomorphism $\phi\colon \mathbb{Z}_3[x]/(f) \to \mathbb{Z}_3[x]/(x-1) \times \mathbb{Z}_3[x]/(x^2+x-1)$. Now observe that the coset representatives in the first component will be constant polynomials a, because all higher powers will be absorbed by the coset. This gives 3 choices for a, meaning that the first component is isomorphic to a group of order 3, and $\mathbb{Z}_3$ is the only group of order 3 up to isomorphism. The coset representatives in the second component will have the form $ax+b$, because all powers higher than 1 will be absorbed by the coset. Thus, we have $3 \cdot 3 = 9$ choices for the coefficients, and thus this set will have size 9. But the second component is also a field, because the coset is a maximal ideal; thus we have that the factor ring is isomorphic to $\mathbb{Z}_3 \times F_9$.

9. a) Let $\mathbb{F}$ be a field and $I \neq \mathbb{F}[x]$ an ideal in $\mathbb{F}[x]$. Suppose I contains an irreducible polynomial f. Show $I = (f) = \{gf \mid g \in F[x]\}$
   b) Use the automorphism $\varphi\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$ given by $\varphi(x) = x+1$ to show $p = x^4 + 1$ is irreducible in $\mathbb{Q}[x]$.
   c) Let $\alpha = \sqrt{i} \in \mathbb{C}$ and $\mathbb{Q}[\alpha] = \{p(\alpha) \mid p \in \mathbb{Q}[x]\} \subseteq \mathbb{C}$. $\mathbb{Q}[\alpha]$ clearly is a subring of $\mathbb{C}$. Use the evaluation map $ev_\alpha\colon \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$ to show $\mathbb{Q}[\alpha]$ is a subfield of $\mathbb{C}$.

Solution:

a) Since I contains f, it follows that $(f) \subseteq I$. Now because f is irreducible over $\mathbb{F}[x]$, it follows that (f) is a maximal ideal, call it J. By the maximality of J, we have for any ideal K containing J that $K = J$ or $K = \mathbb{F}[x]$. Note that I is an ideal containing J but $I \neq \mathbb{F}[x]$; this means that $I = J = (f)$.

b) Observe that under the automorphism, we have that

$$p(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

Now by Eisenstein's Criterion, observe that the prime 2 does not divide 1, but 2 divides every other coefficient and 4 does not divide the constant term; thus we conclude that $p(x+1)$ is irreducible in $\mathbb{Q}[x]$ and thus $p(x)$ is irreducible in $\mathbb{Q}[x]$.

c) Consider the kernel of the evaluation map: we have that Ker $ev_\alpha = \{p \in \mathbb{Q}[x] \mid p(\alpha) = 0\}$. Observe that Ker ev_α contains $x^4 + 1$. As shown previously, this is an irreducible polynomial over $\mathbb{Q}$ and is thus a maximal ideal of $\mathbb{Q}[x]$. Thus, it follows that $\mathbb{Q}[x]/\text{Ker } ev_\alpha$ is a field, but by the First Isomorphism Theorem we have that this is isomorpic to $\mathbb{Q}[\alpha]$; since this is a subring of $\mathbb{C}$ that is also a field, it follows that it is a subfield.

10. a) Let G be a group and N a normal subgroup of G. Show G/N is an abelian group is and only if for all $g, h \in G, ghg^{-1}h^{-1} \in N$.

b) Show the alternating group A_n for $n \geq 5$ has no subgroups H of index strictly less than 5.

Solution:

a) Suppose G/N is abelian. Then we have that $(gN)(hN) = (hN)(gN)$, which means that $ghN = hgN$, meaning that $ghg^{-1}h^{-1}N = N$, so that $ghg^{-1}h^{-1} \in N$. Now suppose that $ghg^{-1}h^{-1} \in N$. Then we have that $ghg^{-1}h^{-1}N = N$, meaning that $ghN = hgN$, so that $(gN)(hN) = (hN)(gN)$, meaning that G/N is abelian.

b) Consider the homomorphism $\varphi\colon A_n \to S(A_n/H)$ wherein the actions of A_n are applied onto the cosets. We have that the right hand side is isomorphic to S_m, where m is the index of H in A_n. By the First Isomorphism Theorem, we have that $A_n/\text{Ker } \varphi$ is isomorphic to a subgroup of S_m. However, observe also that Ker φ is a normal subgroup of A_n, and the fact that A_n is simple means that Ker φ is either A_n or trivial. It cannot be A_n; if it were, taking $x \notin H$ would make $xH \neq H$ so that $\phi(x)$ is not the identity, which contradicts the definition of the homomorphism. Thus Ker φ is trivial and so the factor group has order at least $n!/2 \geq 5!/2 = 60$. But S_m has order strictly less than 60, and there is no way that the factor group of order greater than or equal to 60 could be isomorphic to a group of

order strictly less than 60. This is a contradiction, meaning that no such subgroups of index strictly less than 5 exist.