Suggested solution to the exam in MAT2200 spring 2020

Problem 1. Let $\mu_1 = (1,2)(3,4)$, $\mu_2 = (1,4)(2,3)$ and $\mu_3 = (1,3)(2,4)$ in S_4.

1a. Prove that $N = \{\iota, \mu_1, \mu_2, \mu_3\}$ is a subgroup of S_4. What known group is N isomorphic to? Solution: We compute that $\mu_1^2 = \mu_2^2 = \mu_3^2 = \iota$. We check that the product of two distinct nontrivial elements in N equals the remaining non-trivial element, for example $\mu_1\mu_2 = \mu_3$. We conclude that N is closed under multiplication and is isomorphic to the Klein group V.

1b. Prove that N is a normal subgroup of S_4. Solution: let $\sigma \in S_4$ and a transposition (i,j) be given. For $m \in \{1,2,3,4\}$, the value $\sigma(i,j)(m)$ is $\sigma(j)$ in case $m = i$, it is $\sigma(i)$ in case $m = j$, and is $\sigma(m)$ if m differs from i and j. This matches the result of computing $(\sigma(i), \sigma(j))\sigma(m)$, so we conclude $\sigma(i,j) = (\sigma(i), \sigma(j))\sigma$. Then for disjoint transpositions (i,j) and (k,l) we obtain

$$\sigma(i,j)(k,l)\sigma^{-1} = (\sigma(i,j)\sigma^{-1})(\sigma(k,l)\sigma^{-1}) = (\sigma(i), \sigma(j))(\sigma(k), \sigma(l)),$$

which is again a product of disjoint transpositions. Since σ was arbitrary, it follows that N is a normal subgroup of S_4.

Problem 2.

Let $M_3(F)$ be the ring of 3×3-matrices over a field F. For $a, b, c \in F$ we denote

$$M(a,b,c) = \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(F).$$

Let R be the subset of $M_3(F)$ given by

$$R = \{M(a,b,c) \mid a, b, c \in F\}.$$

2a. Show that R is a subring of $M_3(F)$. Show moreover that R is not commutative and does not contain unity. Solution: Given two elements $M(a,b,c)$, $M(a',b',c')$ in R, their sum is $M(a,b,c) + M(a',b',c') = M(a+a', b+b', c+c')$, so it belongs to R. Their product is $M(aa', ab' + ba', ac')$, so is again in R. Thus R is closed under the operations in $M_3(F)$. The set R contains the additive identity of $M_3(F)$ as the element $M(0,0,0)$, and for each $M(a,b,c) \in R$, its additive identity is $M(-a,-b,-c)$, which is back in R. Thus, R is a subgroup of $M_3(F)$ for the additive structure. The associativity of multiplication is valid in R as a subset of $M_3(R)$, and same for distributivity. We conclude that R is a subring of $M_3(F)$. We notice that the product $M(a',b',c')M(a,b,c,)$ is $M(a'a, a'b+b'a, a'c)$, which differs from $M(a,b,c)M(a',b',c')$, so R is not commutative. It does not contain unity: for a matrix $M(a',b',c')$ to multiply an arbitrary $M(a,b,c)$ back into itself, we need at least $a' = 1, b' = 0$. If $c' = 0$, then $M(1,0,0)$ is not a unity for elements with $c \neq 0$, and no non-zero value of c' can satisfy $ac' = c$ for arbitrary $a, c \in F$.

2b. The multiplication rule from 2a) shows that the map ϕ given by $\phi(M(a,b,c)) = a$ is a ring homomorphism. The same multiplication rules show, for a choice $a \neq c$, that ψ is not a ring homomorphism (since $ac' \neq cc'$).

2c. To see that $I = \{M(a,b,c) \in R \mid a = 0\}$ is an ideal of R, one possibility is to check directly the definition. Other possibility is to note that $I = \ker(\phi)$. The fundamental homomorphism theorem gives that the quotient ring R/I is isomorphic to $\phi[R]$. We see that ϕ is surjective, since for given $a \in F$ we have $\phi(M(a,0,0)) = a$. Thus $\phi[R] = F$, so R/I is a field and thus I is a maximal ideal of R.

Problem 3.

Let G be a group of order $|G| = 1225$.

3a. Show that G has a unique Sylow p-subgroup for each prime p that divides $|G|$. Show that G has two normal subgroups M and N such that the order of M is co-prime with the order of N. Explain why M and N are abelian (you can here use, without proof, a known result from the course). Solution: We have $|G| = 5^2 7^2$. Let N_p be the number of Sylow p-subgroups of G, where $p = 5$ or $p = 7$. By Sylow's theorems, we have $N_p \equiv 1 \pmod p$ and $N_p | 5^2 7^2$. So N_p is of the form $1 + kp$ for $k = 0, 1, 2, \ldots$ and is a divisor of $5^2 7^2$. Verifying the possibilities here we get that $N_5 = 1$ and $N_7 = 1$. Let M be the Sylow 5-subgroup and N be the Sylow 7-subgroup of G. By Sylow's second theorem, each of M and N is a normal subgroup of G. We also have $|M| = 5^2$ and $|N| = 7^2$. Thus the orders of M and N are co-prime. Moreover, by a result in the course, both M and N are abelian, because their order is of form p^2 where p is a prime.

3b. Show that G is isomorphic to the direct product $M \times N$ and conclude it is abelian. Solution: By part 3a, the intersection $M \cap N$ is the trivial subgroup $\{e\}$ of G. Since M and N are normal subgroups of G, we have $xy = yx$ for all $x \in M$ and $y \in N$ by a result in the course. Then the map $f : M \times N \to G$ given by $f(x,y) = xy$ is a homomorphism (easy verification or we can refer to a result in the course). We have $\ker(f) = \{(x,y) \mid x = y^{-1}\} = \{(e,e)\}$ because $M \cap N = \{e\}$, so f is injective. Since $M \times N$ has order equal to the order of G, f is surjective and thus an isomorphism. Since both M and N are abelian, their direct product is abelian, and it follows that G is abelian.

Problem 4. Consider the field $F = \mathbb{Z}_3$ and let $f(x) = x^3 + 2x + 1 \in F[x]$.

4a. Explain why $K = F[x]/\langle f(x)\rangle$ is a field. Solution: K is a field if and only if the ideal $\langle f(x)\rangle$ is a maximal ideal of $F[x]$, which happens precisely when $f(x)$ is irreducible over F. Since the degree of f is at most 3, it suffices to check that $f(x)$ has no zeros in F to conclude it is irreducible over F. Simply check that $f(a) \neq 0$ for all $a \in F$.

4b. We assume known that $K = F(\alpha)$, for $\alpha = x + \langle f(x)\rangle$ in K. Use α to write a basis for K over F. Express α^6 and α^4 in this basis. Solution: The degree of $K = F(\alpha)$ is the degree of the irreducible polynomial $f(x)$ of α over F, so is 3. Thus K has a basis $\{1, \alpha, \alpha^2\}$ over F. Moreover, since α is a zero of $f(x)$, we know $a^3 + 2a + 1 = 0$ in K. From here we get $\alpha^3 = -(2\alpha + 1) = \alpha + 2$, since 2 and 1 are each others additive inverse in F. This gives

$\alpha^4 = \alpha\alpha^3 = \alpha^2 + 2\alpha$ and

$$\alpha^6 = (\alpha + 2)^2 = \alpha^2 + \alpha + 1,$$

since the coefficients are in F.

4c. Find a monic polynomial $g(x)$ of degree 3 in $F[x]$ such that α^2 is a zero of $g(x)$. Solution: Let $g(x) = x^3 + ax^2 + bx + c \in F[x]$ such that $g(\alpha) = 0$. Using 4b, this means,

$$\alpha^2 + \alpha + 1 + a(\alpha^2 + 2\alpha) + b\alpha^2 + c = 0,$$

so $1+c+(1+2a)\alpha+(1+a+b)\alpha^2 = 0$. Since $1, \alpha, \alpha^2$ form a basis for K over F, the coefficients $1 + a + b, 1 + 2a, 1 + c$ are 0 in F. We get the solution $a = b = 1, c = 2$.

4d. Show that $f(1 + \alpha) = 0$ and $f(2 + \alpha) = 0$. Conclude that K is a splitting field of $f(x)$ over F. Solution: Simply insert $1 + \alpha$ and $2 + \alpha$ in $f(x)$ and check that the result is 0. For instance, $f(1+\alpha) = (1+\alpha)^3+2(1+\alpha)+1 = 1+\alpha^3+2\alpha$, since we work over F, and replace α^3 with $\alpha + 2$. Thus K contains the three zeros $\alpha, 1 + \alpha, 2 + \alpha$ of $f(x)$ over F, so it is a splitting field of $f(x)$ over F.

Problem 5.

Let $g(x) = x^3 + 4$ and $f(x) = x^5 + 2x^4 + 3x^3 + 4x^2 + 8x + 12$ in $\mathbb{Q}[x]$. Let L be the splitting field of $g(x)$ over $\mathbb{Q}$ and K the splitting field of $f(x)$ over $\mathbb{Q}$.

5a. Show that $g(x)$ divides $f(x)$ in $\mathbb{Q}[x]$ and that $f(x)$ has no zeros in $\mathbb{Q}$. Solution: Long division shows that $f(x) = g(x)h(x)$, where $h(x) = x^2 + 2x + 3 \in \mathbb{Q}[x]$. None of $g(x)$ or $h(x)$ has zeros in $\mathbb{Q}$ (it suffices to look for zeros in Z, and in fact only check divisors of the constant terms). Thus $f(x)$ has no zeros over $\mathbb{Q}$.

5b. Find L and determine $[L : \mathbb{Q}]$. Solution: The polynomial $g(x)$ has one real zero equal to $\alpha = -\sqrt[3]{4}$ and two conjugate complex zeros $\alpha\zeta$, $\alpha\overline{\zeta}$, where $\zeta = \frac{1+i\sqrt{3}}{2}$. As in Example 50.9 in Fraleigh, we see that $L = \mathbb{Q}(\sqrt[3]{4}, i\sqrt{3})$ by setting up the extension fields $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{4}) \leq (\mathbb{Q}(\sqrt[3]{4}))(i\sqrt{3})$. Then

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{4})][\mathbb{Q}(\sqrt[3]{4}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

5c. Prove that $[K : L] = 2$ and determine $[K : \mathbb{Q}]$. Explain why K is a finite normal extension of $\mathbb{Q}$. Solution: The field K contains all the zeros of $f(x)$ over $\mathbb{Q}$, so it contains L as a subfield. The zeros of $h(x)$ in $\mathbb{C}$ are $-1 \pm i\sqrt{2}$.

We claim that $K = \mathbb{Q}(\sqrt[3]{4}, i\sqrt{2}, i\sqrt{3})$ (by definition, the splitting field of $f(x)$ over $\mathbb{Q}$ is the smallest subfield of $\overline{\mathbb{Q}}$ containing all the zeros of $f(x)$). We claim that $i\sqrt{2} \notin L$. If $i\sqrt{2} \in \mathbb{Q}(\sqrt[3]{4})$, then $\deg(i\sqrt{2}, \mathbb{Q})$ divides $\deg(\sqrt[3]{4}, \mathbb{Q})$, in other words 2 (the degree of $x^2 + 2$) divides 3, a falsity. So, $i\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{4})$. If $i\sqrt{2} \in \mathbb{Q}(i\sqrt{3})$, then $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$, so $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{3})$, which would imply $\deg(\sqrt{2}+\sqrt{3}, \mathbb{Q})$ divides $\deg(\sqrt{3}, \mathbb{Q})$, a falsity since 4 does not divide 2. So, $i\sqrt{2} \notin \mathbb{Q}(i\sqrt{3})$. Since L is the smallest subfield of $\overline{\mathbb{Q}}$ containing $\sqrt[3]{4}$ and $i\sqrt{3}$, we get $i\sqrt{2} \notin L$. We conclude that

$$K = \mathbb{Q}(\sqrt[3]{4}, i\sqrt{3}, i\sqrt{2}) = L(i\sqrt{2}).$$

Further, $[K : L] = \deg(i\sqrt{2}, L) = 2$. By the product formula for degrees, we get $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 2 \cdot 6 = 12$.

Clearly each of $\sqrt[3]{4}, i\sqrt{2}, i\sqrt{3}$ is separable over $\mathbb{Q}$. Thus K is a separable extension over $\mathbb{Q}$ and since it is a finite extension over $\mathbb{Q}$ and a splitting field over $\mathbb{Q}$, it is a finite normal extension over $\mathbb{Q}$.

5d. Explain why $G(K/L)$ is a normal subgroup of the Galois group $G(K/\mathbb{Q})$. Solution: The Galois correspondence between intermediate subfields $\mathbb{Q} \leq E \leq K$ and subgroups $G(K/E)$ of $G(K/\mathbb{Q})$ satisfies properties 1-6 in the Main Theorem of Galois theory. Therefore $G(K/L)$ is a normal subgroup of the Galois group $G(K/\mathbb{Q})$ if and only if L is a normal extension of $\mathbb{Q}$. But L is a separable splitting field over $\mathbb{Q}$ and a finite extension, so indeed L is a (finite) normal extension of $\mathbb{Q}$, as needed.

Show that $G(K/\mathbb{Q})$ contains a normal subgroup N of order 6, and that $G(K/\mathbb{Q})$ is the direct product of N and $G(K/L)$. Solution: Since the Galois correspondence is bijective, a subgroup $G(K/E)$ of the Galois group $G(K/\mathbb{Q})$ of order 6 must correspond to an intermediate extension $\mathbb{Q} \leq E \leq K$ such that $[K : E] = 6$. We see that $E = \mathbb{Q}(i\sqrt{2})$ is such an extension: clearly $[E : \mathbb{Q}] = 2$, so $[K : E] = 6$ holds by the product formula for the degree using an intermediate extension. Let $N = G(K/E)$. Then N has index $[E : \mathbb{Q}] = 2$ as a subgroup of $G(K/\mathbb{Q})$, so it is a normal subgroup. An element in N is an automorphism of K fixing $i\sqrt{2}$, and an element of $G(K/L)$ is an automorphism of K fixing $\sqrt[3]{4}$ and $i\sqrt{3}$, thus the intersection of N and $G(K/L)$ consists of the identity automorphism of K. As in problem 3b, we obtain that $G(K/\mathbb{Q})$ is isomorphic to the direct product of its normal subgroups N and $G(K/L)$.