Answers to the exam problems in MAT2200 spring 2021

Problem 1a. Use the axioms for a group: the set is closed under matrix multiplication because $aa' \in \mathbb{Z}_6^*$ when $a, a' \in \mathbb{Z}_6^*$ and contains the identity matrix. Since

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for $a' = a^{-1}$ in $\mathbb{Z}_6^*$ and $b' = -a^{-1}b$, every element has an inverse in G. Associativity of multiplication in G holds because it holds in the ring $M_2(R)$ of 2×2 matrices over any ring R. Multiplication is not commutative, as for example

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

The order of the group is $2 \times 6 = 12$.

Problem 1b. An element of order three must satisfy $a^3 = 1$ in $\mathbb{Z}_6^*$, and since $\mathbb{Z}_6^* = \{1, 5\}$ we need $a = 1$. Since the k'th power of a matrix with $a = 1$ and b in entry $(1, 2)$ has entry kb in that entry, we need $3b \equiv 0 \pmod 6$, which gives the possibilities $b = 2$ and $b = 4$. In all we have 2 elements of order 3.

By Sylow's theorems applied to G of order p^2q with $p = 2$ and $q = 3$ give the possibilities $N_2 \equiv 1 (\text{mod } 2)$ and N_2 divides the index 3 of any Sylow 2-subgroup and, similarly, $N_3 \equiv 1 (\text{mod } 3)$ and N_3 divides the index 4 of any Sylow 3-subgroup. Thus N_2 is 1 or 3 and N_3 is 1 or 4. We can exclude $N_3 = 4$ since there are only two elements of order three, so $N_3 = 1$ and the Sylow 3-subgroup is normal by Sylow's second theorem.

Alternatively, the element with $a = 1$, $b = 5$ has order 6 in G so it generates a cyclic subgroup of index 2, which is necessarily normal.

Problem 2a. For G a cyclic group of order n and $1 \leq d \leq n$ a divisor, there is a unique subgroup H of G of order d. If x is a generator of H, all other generators have form x^k where $gcd(k, d) = 1$, thus there are $\phi(d)$ elements of order d in G (also proved during the course). We have that G partitions into the sets $G_d = \{x \mid x \in G, |x| = d\}$ for every divisor d of n, and this implies the claimed equality.

Problem 2b. Assume G is a finite group of order n such that for each divisor d of n there is at most one subgroup of G of order d. By Lagrange's theorem, the order $|x|$ of an arbitrary x in G divides n, and we have that G partitions into the (disjoint) sets G_d as d varies over divisors of n, possibly with G_d empty. If some G_d is non-empty, then an element $x \in G_d$ generates a subgroup $\langle x \rangle$ of G of order d, and this is the only subgroup of order d by assumption. Then $G_d = \{y \in G \mid \langle y \rangle = \langle x \rangle\}$, thus G_d consists of all the elements in G that generate the cyclic group $\langle x \rangle$. A cyclic group of order d has $\phi(d)$ generators. It follows that the number of elements of G_d for d a divisor of n is at most $\phi(d)$. From $n = \sum_{d|n} |G_d| \leq \sum_{d|n} \phi(d) = n$ we get $|G_d| = \phi(d)$ for each divisor d of n, so G_n is non-empty and any of its elements generates G.

Problem 3a. We see that $x^4+1=(x^2+1)^2$ in $\mathbb{Z}_2[x]$, so it is not irreducible and its principal ideal $\langle x^4+1\rangle$ is not prime (it does not contain the factor x^2+1, a polynomial of lower degree than 4, by the division algorithm).

Problem 3b. To show $f(x)=x^4+x^3+1$ is irreducible in $\mathbb{Z}_2[x]$ we first note that there are no zeros in $\mathbb{Z}_2$, as $f(0)=1=f(1)$. Then we see that a factorisation $(x^2+ax+b)(x^2+cx+d)$ forces $b=d=1$ and leads to $1=a+c=0$, an absurdity. The ideal $\langle f(x)\rangle$ is maximal in $\mathbb{F}_2[x]$, hence the quotient ring $\mathbb{F}_2[x]/\langle f(x)\rangle$ is a field extension of $\mathbb{F}_2$ of degree 4, the degree of $f(x)$. Thus there exists θ in the quotient field which is a zero of $f(x)$. Since $\mathbb{F}_2[x]/\langle f(x)\rangle$ is a field with basis $\{1,\theta,\theta^2,\theta^3\}$ over $\mathbb{F}_2$, it has 16 elements. But $\mathbb{F}_{2^4}$ is the unique field with 2^4 elements, up to isomorphism, so we can identify $\mathbb{F}_2[x]/\langle f(x)\rangle$ and $\mathbb{F}_{2^4}$.

To see that the polynomial is primitive, we compute powers θ^j and see that the lowest such that $\theta^j=1$ is $j=15$. This is the order of the cyclic group $\mathbb{F}_{2^4}^*$, so $f(x)$ is a primitive polynomial. We can use the feedback shift register, or note that neither of θ^3 and θ^5 equals 1, with $3,5$ the possible orders of subgroups of $\mathbb{F}_{2^4}^*$ (by Lagrange's theorem or the structure of subgroups of cyclic groups).

Problem 3c. Since x^4+x+1 is irreducible in $\mathbb{F}_2[x]$, a similar argument to the one in part 3b gives that the quotient field $\mathbb{F}_2[x]/\langle x^4+x+1\rangle$ is isomorphic to $\mathbb{F}_{2^4}$. Since a composition of isomorphisms of fields is again an isomorphism of fields, we get that the two quotient fields in the problem are isomorphic.

Problem 3d. Since $f(x)=x^4+x^3+1$ is irreducible of degree 4, it divides $x^{16}-x$. Then $\mathbb{F}_{16}$ is a splitting field of $f(x)$ over $\mathbb{F}_2$. Alternatively, since $\mathbb{F}_{2^4}$ contains a zero θ of the irreducible polynomial $f(x)$ over $\mathbb{F}_2$, it must contain all zeros of $f(x)$. We find them as $\sigma_2(\theta)=\theta^2$, $\sigma_2^2(\theta)=\theta^4$ and $\sigma_2^3(\theta)=\theta^8$. Thus a splitting of $f(x)$ in $\mathbb{F}_{2^4}$ is $f(x)=(x-\theta)(x-\theta^2)(x-\theta^4)(x-\theta^8)$.

Problem 4a. We have $\pm\sqrt{2}$ and $\pm\sqrt{5}$ are the zeros of $f(x)$ in $\mathbb{C}$. The required splitting field is $K=\mathbb{Q}(\sqrt{2},\sqrt{5})$, which is seen to be separable over Q since each of $\sqrt{2}$ and $\sqrt{5}$ is separable over $\mathbb{Q}$. To compute the degree use the intermediate formula on

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt{5}).$$

The leftmost extension is of degree 2, since x^2-2 is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. The rightmost extension cannot have degree 1 because otherwise $\beta=\sqrt{2}+\sqrt{5}$ is in $\mathbb{Q}(\sqrt{2})$; however, $(\beta-\sqrt{2})^2=5$ leads to β being a zero of x^4-14x^2+9, which is monic and irreducible over $\mathbb{Q}$. Thus

$$2=[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2}):\mathbb{Q}(\beta)][\mathbb{Q}(\beta):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2}):\mathbb{Q}(\beta)]\cdot 4,$$

which is absurd. So $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}(\beta)]>1$ and since it is at most 2 because $\sqrt{5}$ is a zero of $x^2-5\in\mathbb{Q}(\sqrt{2})[x]$ this degree must be 2. In all, $[K:\mathbb{Q}]=4$.

Problem 4b. By part 4a, K is a finite normal extension of $\mathbb{Q}$. The Galois group $Gal(K/\mathbb{Q})$ has order 4. As in lecture 30, we find three elements of order 2 in $Gal(K/\mathbb{Q})$: these are the conjugation automorphisms $\sigma=\psi_{\sqrt{2},-\sqrt{2}}$, $\eta=\psi_{\sqrt{5},-\sqrt{5}}$ and $\tau=\psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{5},-\sqrt{5}}$. Thus $Gal(K/\mathbb{Q})$ is isomorphic to the Klein group V.

To determine the fixed fields corresponding to the three proper non-trivial subgroups of $Gal(K/\mathbb{Q})$, we first obtain that $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ is a basis for K over $\mathbb{Q}$ by the proof of the degree formula for intermediate field extensions, so

$$K = \{a_0 + a_1\sqrt{2} + a_2\sqrt{5} + a_3\sqrt{10} \mid a_0, \ldots, a_3 \in \mathbb{Q}\}.$$

We compute the fixed field E_H for the subgroup H of $Gal(K/\mathbb{Q})$ generated by η: it is determined by

$$a_0 + a_1\sqrt{2} + a_2\sqrt{5} + a_3\sqrt{10} = a_0 + a_1\sqrt{2} - a_2\sqrt{5} - a_3\sqrt{10},$$

thus requires $a_2 = a_3 = 0$ by linear independence of the basis. Thus the required subfield of K is $\{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}\}$, which is isomorphic to $\mathbb{Q}(\sqrt{2})$. Similar computations (details required at exam) show that the subgroup generated by σ has fixed field $\mathbb{Q}(\sqrt{5})$ and the subgroup generated by $\sigma \circ \eta$ has fixed field $\mathbb{Q}(\sqrt{10})$.