MTHM024/MTH714U Group Theory

Problem Sheet 5 Solutions

---

1 (a) We construct $\mathbb{F}_8$ by adjoining to $\mathbb{F}_2 = \mathbb{Z}_2$ the root of an irreducible cubic polynomial $f(x)$.

> The reason for this is that, if f is irreducible, then the ideal $\langle f \rangle$ of the polynomial ring $\mathbb{F}_2[x]$ generated by f is maximal, and hence the quotient ring $\mathbb{F}_2[x]/\langle f \rangle$ is a field (see Algebraic Structures II notes). Now the Division algorithm shows that, if p is any polynomial over $\mathbb{F}_2$, then we can write $p(x) = f(x)q(x) + r(x)$, where $\deg(r) < \deg(f) = 3$, so r belongs to the coset $\langle f \rangle + p$. Thus every coset contains a representative of degree less than 3. It is easy to see that this coset representative is unique. The number of polynomials of degree less than 3 is $2^3 = 8$ (since $ax^2 + bx + c$ has three coefficients each of which can be any element of $\mathbb{F}_2$). So there are 8 cosets of $\langle f \rangle$ in $\mathbb{F}_2[x]$, and the quotient is a field with 8 elements.
>
> We note in passing that, if we use the symbols $0, 1, \alpha$ to denote the cosets $\langle f \rangle$, $\langle f \rangle + 1$ and $\langle f \rangle + x$ respectively, then $f(\alpha) = \langle f \rangle + f(x) = \langle f \rangle = 0$. Thus α is a root of f.

There are eight polynomials of degree 3 over $\mathbb{F}_2$. If f is an irreducible polynomial of degree 3, then $f(0) = 1$ (since if $f(0) = 0$ then x is a factor of $f(x)$), and $f(1) = 1$ (since if $f(1) = 0$ then $x + 1$ is a factor of $f(x)$). This leaves just the two irreducible polynomials $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$.

Now take the polynomial f. The eight elements of our field are $a\alpha^2 + b\alpha + c$, where $a, b, c \in \mathbb{F}_2$ and $\alpha^3 + \alpha + 1 = 0$. Addition is straightforward: to add two expressions of this form, we simply add the coefficients of α^2, the coefficients of α, and the constant terms. For example, $(\alpha^2 + 1) + (\alpha^2 + \alpha) = \alpha + 1$.

Multiplication can be done by multiplying in the usual way and using the fact that $\alpha^3 = \alpha + 1$ to reduce the degree of the product. A more user-friendly way to multiply is to use "logarithms". We construct a table of powers of α:

α^0					1
α^1			α		
α^2	α^2				
α^3			α	$+$	1
α^4	α^2	$+$	α		
α^5	α^2	$+$	α	$+$	1
α^6	α^2			$+$	1

and $\alpha^7 = 1 = \alpha^0$. So the multiplicative group is cyclic of order 7, in agreement with what we know.

Now to multiply two elements, use the table to express them as powers of α, add the exponents mod 7, and use the table in reverse to express the result in the standard form. For example,

$$(\alpha^2+1)(\alpha^2+\alpha) = \alpha^6 \cdot \alpha^4 = \alpha^{10} = \alpha^3 = \alpha + 1.$$

(b) Let $\beta = \alpha^3$. (Why this choice? Trial and error – see below.) Then

$$\beta^3 + \beta^2 + 1 = \alpha^9 + \alpha^6 + 1 = \alpha^2 + (\alpha^2+1) + 1 = 0,$$

so β is a root of the other irreducible polynomial g. So the field we construct already contains a root of g, and thus is the field obtained by adjoining such a root to $\mathbb{F}_2$. So the two irreducible polynomials give the same field.

If you try $\gamma = \alpha^2$, you will find that $f(\gamma) = 0$, so γ is a root of the same irreducible polynomial as is α. In fact, this agrees with our observation that the *Frobenius map* $u \mapsto u^2$ is an automorphism of $\mathbb{F}_8$. Similarly, α^4, the result of applying the Frobenius map twice, will also satisfy f. The other two elements $\alpha^6 = (\alpha^3)^2$ and $\alpha^5 = (\alpha^3)^4$ are roots of g.

2 (a) The following are equivalent (for $g \in G$):

- Hg is fixed by H,
- $(Hg)h = Hg$ for all $h \in H$,
- $Hghg^{-1} = H$ for all $h \in H$,
- $ghg^{-1} \in H$ for all $h \in H$,
- $gHg^{-1} = H$,

- $g^{-1}Hg = H$.

(b) Let $H = p^k$. Then the coset space $\cos(H,G)$ has size p^{n-k}, a multiple of p (since $H < G$). Now consider the action restricted to H, and split $\cos(H,G)$ into orbits. By the Orbit-Stabiliser Theorem, the size of each orbit is a power of p; and at least one orbit (namely $\{H\}$) has size $1 = p^0$. So there must be at least p orbits of size 1; that is, at least p cosets of H lie in $N_G(H)$, by (a). So $N_G(H) > H$.

3 The first part asks, which matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfy $A^2 = I$ and $\det(A) = 1$? We have $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = A$; so $b = -b$, $c = -c$, $a = d$. Since the characteristic of the field is not 2, we conclude that $b = c = 0$ and $A = aI$. Then $a^2 = 1$, so $a = -1$, as required.

(a) $\mathrm{PSL}(2,F)$ contains an involution; indeed, it is easy to see that it contains more than one involution. (For example, thinking of it as the group of linear fractional transformations, $z \mapsto -a^2 z$ is an involution for any non-zero $a \in F$, so if $|F| > 3$ there is more than one such element. The case $|F| = 3$ can be handled directly.) So it cannot be a subgroup of a group with only one involution. [An *involution* is an element of order 2.]

(b) Since the composition factors are C_2 and $\mathrm{PSL}(2,q)$, and there is no subgroup (normal or otherwise) isomorphic to $\mathrm{PSL}(2,q)$, the composition series must be $G \rhd H \rhd \{1\}$, where $H \cong C_2$. By the first part of the question, there is only one such subgroup H, namely $\{\pm I\}$.

(c) Immediate from (a) (or (b)).

4 (a) First observe that a conjugate of a p-th power or a commutator is again a p-th power or commutator respectively — we have $(x^p)^g = (x^g)^p$ and $[x,y]^g = [x^g, y^g]$, where $x^g = g^{-1}xg$ and $[x,y] = x^{-1}y^{-1}xy$ [you should check this!]. So conjugation maps the generators of N to themselves, and hence fixes N. Thus it is a normal subgroup.

For any elements $x, y \in G$, we have $(Nx)^p = Nx^p = N$ and $[Nx, Ny] = N[x,y] = N$. So G/N is a group in which every p-th power and every commutator is the identity, in other words, it is an elementary abelian p-group.

(b) Let K be a normal subgroup of G such that G/K is an elementary abelian p-group. Choose any elements $x, y \in G$. Then $(Kx)^p = Kx^p = K$, so $x^p \in K$; and $[Kx, Ky] = K[x,y] = K$, so $[x,y] \in K$. Thus all the generators of N lie in K, and so $N \leq K$.

(c) Let H be a maximal subgroup of G. By Problem 2(b), $N_G(H) > H$. Hence by maximality we have $N_G(H) = G$, that is, $H \lhd G$. Now since H is a maximal subgroup of G, G/H is a group whose only subgroups are itself and the identity; so necessarily $G/H \cong C_p$, and $|G:H| = p$.

(d) Let H be a maximal subgroup of G. By part (c), $H \lhd G$ and $G/H \cong C_p$. Hence by part (b), $N \leq H$. So $N \leq M$, where M is the intersection of all maximal subgroups of G.

Now G/N is elementary abelian, that is, the additive group of a vector space over $\mathbb{F}_p$, whose subspaces are subgroups of G/N. According to the Correspondence Theorem, M/N is a subgroup of G/N, hence a subspace of this vector space. Suppose for a contradiction that $M \neq N$. Then $M/N \neq \{0\}$. Choose a subgroup K such that $(M/N) \oplus (K/N) = G/N$ (using the Correspondence Theorem again). This means that, in group terms, $MK = G$.

By assumption, $K \neq G$. So K is contained in a maximal subgroup H of G. By assumption, $M \leq H$ (since M is the intersection of all the maximal subgroups). As $M \leq H$ and $K \leq H$, we have $G = MK \leq H$, which is an obvious contradiction. So necessarily, $M = N$, as required.

(e) Suppose that $Ng_1, \ldots, Ng_r$ generate G/N, and suppose for a contradiction that $g_1, \ldots, g_r$ don't generate G. The subgroup they do generate is contained in some maximal subgroup H of H. Thus $g_1, \ldots, g_r \in H$. But also $N \leq H$, by part (d). This means that $Ng_1, \ldots, Ng_r \in H/N$, contradicting the fact that they generate G/N. So the assertion is proved.

Remark The subgroup N is called the *Frattini subgroup* of G. The result that the number of generators of G is equal to the dimension of G/N as a vector space over $\mathbb{F}_p$ is called the *Burnside basis theorem*.