Homework7 Yiwei Yang 2018533218

1

Let K be the subfield of F. F is a vector space over K, finite-dimensional since F is finite. Denote this dimension by m. Then F has a basis over K consisting of m elementes. let it be $b_1, b_2 ... b_m$. Every element of F can be uniquely represented in the form $k_1 b_1 + ... k_m b_m$(where $k_1, ... k_m \in K$) Since each $k_i \in K$ can take q values. Then F must have exactly q^m elements.□

2

i

Lemma

Let $g \in G$ and g have order n. Then $g^k = e$ if and only if $n \mid k$.
If $n \mid k$, say $k = nm$, then $g^k = g^{nm} = (g^n)^m = e$. For the converse direction, we use the division theorem. Supposing that $g^k = e$, write $k = nq + r$ with integers q and r such that $0 \leq r < n$. Then

$$e = g^k = (g^n)^q g^r = g^r \tag{1}$$

Since $0 \leq r < n$, the minimality built into n as the order of g forces r to be zero. Thus $k = nq$, so $n \mid k$

Proof

From the problem we have g_1 has order n_1 and g_2 has order n_2, with $(n_1, n_2) = 1$, we are to proof g_1, g_2 has order n_1, n_2. Since

$$(g_1 g_2)^{n_1 n_2} = g_1^{n_1 n_2} g_2^{n_1 n_2} = (g_1^{n_1})^{n_2} (g_2^{n_2})^{n_1} = e \tag{2}$$

we see $g_1 g_2$ has finite order, which must divide $n_1 n_2$ by Theorem 3.4. Let n be the order of $g_1 g_2$. In particular, $(g_1 g_2)^n = e$. From this we will show $n_1 \mid n$ and $n_2 \mid n$. Since g_1 and g_2 commute,

$$g_1^n g_2^n = e \tag{3}$$

Raising both sides of $g_1^n g_2^n = e$ to the power n_2 (to kill off the g_2 factor) gives

$$g_1^{n n_2} = e \tag{4}$$

Therefore $n_1 \mid n n_2$ by Lemma. Since $(n_1, n_2) = 1$, we conclude $n_1 \mid n$. Now raising both sides of $g_1^n g_2^n = e$ to the power n_1 gives $g_2^{n n_1} = e$, so $n_2 \mid n n_1$ by Lemma, and thus $n_2 \mid n$
Since $n_1 \mid n, n_2 \mid n$ and $(n_1, n_2) = 1$, we conclude that $n_1 n_2 \mid n$. Since we already showed $n \mid n_1 n_2$ (in the first paragraph of the proof), we conclude $n = n_1 n_2$.□

ii

The proposition can be extended to a more general one. If F is a field and G a finite subgroup of $F^{\times}$, then G is cyclic. This follow from the same hint: With $n = |G|$, we have $g^n = 1$ for all $g \in G$, hence all $g \in G$ are roots of the polynomial $X^n - 1 \in F[X]$.

Since there are at most n such roots, the elements of G are precisely the n roots of the polynomial $X^n - 1$. Now let g be a root of $X^n - 1$, but not of $X^d - 1$ for any $d \mid n$

Then clearly $G = \langle g \rangle. \square$

3

i

Cite the algorithm from https://jtnb.centre-mersenne.org/article/JTNB_2015__27_1_245_0.pdf
$P(x, y) = xy - y^2$
Check:
The latter is obviously satisfied.
For first equation: if $X = Y - 1, P(x, y) = y^2 - y - y^2 \ (mod\ y - 1) \equiv 1$

ii

$n_1 = 7$
$n_2 = 16$
$n_3 = 10$
$N = n_1 \cdot n_2 \cdot n_3 = 1120$
$m_1 = \frac{N}{n_1} = 160$
$m_2 = \frac{N}{n_2} = 70$
$m_3 = \frac{N}{n_3} = 112$
$\gcd(m_1, n_1) = \gcd(160, 7) = 1$ so $y_1 = 1$ and $x_1 = 160$
$\gcd(m_2, n_2) = \gcd(70, 16) = 2$ so $y_2 = 2$ and $x_2 = 70$
$\gcd(m_3, n_3) = \gcd(112, 10) = -2$ so $y_3 = -2$ and $x_3 = -112$

So $x = 160 \times 3 + 70 \times 4 - 112 \times 2 \equiv 584 (\bmod 1120)$

4

These are dihedral group:D8 and quaternion group

First let generalize the problem, let 8 be any prime number p^3.

Lemma

Given: A prime number p, a group P of order p^3.
To prove: Either P is abelian, or we have: $Z(P)$ is a cyclic group of order p and $P/Z(P)$ is an elementary abelian group of order p^2
Proof: Let $Z = Z(P)$ be the center of P.
P has order p^3, specifically, a power of a prime, so Z is non trivial. P has order p^3, P/Z exists by

the fact that center is normal and has order $|P|/|Z|$ by Lagrange's theorem. If Z has order p^2, the order of P/Z is $p^3/p^2 = p$. By the quaivalence of definitions of group of prime order, P/Z must be cyclic. Then, by the fact that cyclic over central implies abelian, P would be abelian, but this would imply that $Z = P$, in which case the order of Z would have been p^3. So, the order of Z can not be p^2

By Lagrange's theorem, the order of Z must divide the order of P. The only possibilities are $1, p, p^2, p^3$. Step the frist process eliminates the possibility of 1 , and the second process eliminates the possibility of p^2. This leaves only p or p^3.

If Z has order p, then Z must be cyclic. P/Z exists and its order is $|P|/|Z| = p^3/p = p^2$. P/Z cannot be cyclic, because if it were cyclic, then P would be abelian, which would mean that $Z = P$ has order p^3. Thus, P/Z is a non-cyclic group of order p^2. By classification of groups of prime-square order, the only non-cyclic group of order p^2 is the elementary abelian group, so P/Z must be the elementary abelian group of order p^2. If Z has order p, then Z is cyclic of order p and the quotient P/Z is elementary abelian of order p^2

If Z has order p^3, we get $P = Z, P$ is abelian.

Classifying the non-abelian groups

Case A: a and b both have order p.
In this case, the relations so far give the presentation:
$\langle a, b, z \mid a^p = b^p = z^p = e, az = za, bz = zb, [a, b] = z\rangle$
These relations already restrict us to order at most p^3, because we can use the commutation relations to express every element in the form $a^\alpha b^\beta z^\gamma$, where α, β, γ are integers mod p. To show that there is no further reduction, we note that there is a group of order p^3 satisfying all these relations, namely unitriangular matrix group:UT (3,p). This is the multiplicative group of unipotent upper-triangular matrices with entries from the field of p elements. Thus, Case A gives a unique isomorphism class of groups. Note that the analysis so far works both for $p = 2$ and for odd primes. The nature of the group obtained, though, is different for $p = 2$, where we get dihedral group:D8 which has exponent p^2. For odd primes, we get a group of prime exponent.

Case B: a has order p^2, b has order p In this case, we first note that $a^p \in Z = \langle z\rangle$. Since a^p is a non-identity element, there exists nonzero r (taken mod p) such that $a^p = z^r$. Consider the element $c = b^r$ Then, by Fact thatClass two implies commutator map is endomorphism, and the observation that P has class two (Step (1) in the above table), we obtain:
$[a, c] = [a, b^r] = [a, b]^r = z^r = a^p$
Consider the presentation:
$\left\langle a, c \mid a^{p^2} = c^p = e, [a, c] = a^p \right\rangle$
We see that all these relations are forced by the above, and further, that this presentation defines a group of order p^3, namely semidirect product of cyclic group of prime-square order and cyclic group of prime order.
Thus, there is a unique isomorphism class in Case B. Note that the analysis so far works both for $p = 2$ and for odd primes. The nature of the group, though, is different for $p = 2$, we get dihedral group:D8, which is the same isomorphism class as Case A.

Case B2: a has order p, b has order p^2. Interchange the roles of a, b and replace z by z^{-1} and we are back in Case B.

Case C: a and b both have order p^2.
By Fact that Formula for powers of product in group of class two, we can show that for odd prime, it is possible to make a substitution and get into Case B.
For $p = 2$, working out the presentation yields quaternion group.
Here is a summary of the cases: