

Mathematics 504 Autumn 2003

1. Show that any finite abelian group is isomorphic to the direct product of its Sylow subgroups (without using the fundamental theorem of finitely generated abelian groups).

Comments. I have three comments about this problem. First, if you want to proceed by induction (which I think is a natural choice), then you need to justify why, if G has order $p_1^{i_1} \dots p_n^{i_n}$, there is a subgroup of order $p_1^{i_1} \dots p_{n-1}^{i_{n-1}}$. I gave one explanation in the solutions; a variant on that approach would be to let P_i be the Sylow p_i -subgroup of G , and let $H = P_1 P_2 \dots P_{n-1}$. Then you have to say why H is a subgroup, and you have to compute its order.

Second, I think any solution to this problem will use the “recognition theorem” for direct products. There was a little confusion about the statement of this theorem, probably because of how it’s stated in the book. Given subgroups H and K of G , if you can show that H and K are each normal, and that $H \cap K = \{1\}$, then you can only conclude that $HK \cong H \times K$. If you want to show that $G \cong H \times K$, then you also need to show that $G = HK$.

Finally, several people were tempted to try to use the obvious generalization of this recognition theorem with more than two factors. Unfortunately, the “obvious” generalization is false: suppose you have a group G and subgroups H_1, H_2, \dots, H_n . Suppose also that

- H_i is normal in G for each i ,
- $H_i \cap H_j = \{1\}$ for all distinct i and j .
- $H_1 H_2 \dots H_n = G$.

Then G need not be isomorphic to $H_1 \times \dots \times H_n$. For example, let G is the Klein 4-group:

$$G = \{1, a, b, ab : a^2 = b^2 = 1, ab = ba\}.$$

Let $H_1 = \{1, a\}$, $H_2 = \{1, b\}$, $H_3 = \{1, ab\}$. Then these subgroups satisfy the above conditions, but G is not isomorphic to $H_1 \times H_2 \times H_3 \cong C_2 \times C_2 \times C_2$.

I *think* that a recognition theorem for products of more than two factors would require that

- H_i is normal in G for each i ,
- $H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_n = \{1\}$ for all i ,
- $H_1 H_2 \dots H_n = G$.

It’s probably easier to use induction in any specific case; showing the second condition will require induction anyway, I would think.

2. If K/F is an abelian Galois extension of degree $540 = 2^2 \times 3^3 \times 5$, what are the possible Galois groups? Among all such extensions, what is the maximum number of intermediate fields E such that $[K : E] = 2$? What is the minimum number?

Comments. I just want to emphasize the statement of the fundamental theorem of Galois theory: in the bijection between intermediate fields E and subgroups H of the Galois group, the *order* of H equals the degree $[K : E]$. (You may be able to remember this by considering the cases $E = K$, in which case $[K : E]$ is clearly 1, and $E = F$, in which case $[K : E] = |G|$.)

3. Assume that G is a group of order $231 = 3 \times 7 \times 11$. Show that G contains a normal Sylow 7-subgroup and a central Sylow 11-subgroup.

Comments. A few people ignored the word “central” and just showed that there is a normal Sylow 11-subgroup. (More people got stuck on the centrality part – see the solutions for one approach.)

4. Let p be a prime and n a positive integer. Use the fundamental theorem of Galois theory and facts about the extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ to classify the subfields of \mathbf{F}_{p^n} .

Comments. Since the problem asks you to classify the subfields of \mathbf{F}_{p^n} , and since Galois theory lets you classify the fields F with $\mathbf{F}_p \subseteq F \subseteq \mathbf{F}_{p^n}$, you should explain why these are the same problem – why every subfield of \mathbf{F}_{p^n} contains \mathbf{F}_p . I don’t think anyone did this (except me, in the solutions).

Also, some of you only did half of the problem: you showed that if F was a subfield of \mathbf{F}_{p^n} , then $F = \mathbf{F}_{p^d}$ for some d dividing n . You also need to do the converse: if $d \mid n$, then \mathbf{F}_{p^d} is in fact a subfield of \mathbf{F}_{p^n} . (The fundamental theorem of Galois theory allows you to do the whole thing all at once.)

Finally, the Galois correspondence threw some of you off: a subgroup of order d of the Galois group corresponds to a field F with $[\mathbf{F}_{p^n} : F] = d$, and so with $[F : \mathbf{F}_p] = n/d$. So the field corresponding to the cyclic group C_d is the field $\mathbf{F}_{p^{n/d}}$.

5. Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. Let K be the splitting field of $p(x)$. Show that the Galois group $G = \text{Gal}(K/F)$ acts transitively on the roots of $p(x)$. (For full credit, do this without using the fundamental theorem of Galois theory.)

Comments. The word “transitively” was misunderstood by some of you. If you show that, whenever α is a root and $\sigma \in G$, then $\sigma(\alpha)$ is a root, you have showed that G permutes the roots. This is part of the problem. The rest is to show that the action is *transitive*: for any two roots α and β , there is an element σ of G so that $\sigma(\alpha) = \beta$.

One possible approach to this problem is to use the theorem about extending isomorphisms: given two roots α and β of $p(x)$, the fields $F(\alpha)$ and $F(\beta)$ are isomorphic: there is an isomorphism $\phi : F(\alpha) \rightarrow F(\beta)$. So by some theorem, you can extend this isomorphism: there is a field K' and an isomorphism $\psi : K \rightarrow K'$ like this:

$$\begin{array}{ccc}
 K & \xrightarrow{\psi} & K' \\
 \downarrow & & \downarrow \\
 F(\alpha) & \xrightarrow{\phi} & F(\beta) \\
 \downarrow & & \downarrow \\
 F & \xlongequal{\quad} & F
 \end{array}$$

To finish the problem, you then have to show that $K' = K$ (not just that they’re isomorphic, but actually equal).

If you want to use an extension theorem, you can proceed as follows: one extension theorem says this: given $f(x) \in F[x]$, and given an isomorphism $F \xrightarrow{\varphi} F'$, let K be the splitting field of $f(x)$, and let K' be the splitting field of $\varphi(f(x))$. Then there is an extension of the isomorphism φ to $\psi : K \rightarrow K'$. To apply this to our problem, let α and β be roots of $p(x)$. Then there is an isomorphism $F(\alpha) \xrightarrow{\varphi} F(\beta)$ which fixes F , and hence fixes $p(x)$. Now note that K is the splitting field of $p(x) \in F(\alpha)[x]$, and it is also the splitting field of $p(x) \in F(\beta)[x]$; therefore by the theorem, there is an isomorphism $K \xrightarrow{\psi} K$ extending the isomorphism φ .

6. Let K/F be a field extension, and fix $a \in K$. Show that $F(a)$ is algebraic over F if and only if $[F(a) : F]$ is finite. Use this to prove that sums, differences, products, and quotients of algebraic elements are algebraic.

Comments. Note that part of what you should show is that if $[F(a) : F]$ is finite, then the *field* $F(a)$ is algebraic over F : every element of $F(a)$ is algebraic over F . I didn't take off any points if you just showed that a is algebraic. (It's true that the field $F(a)$ is algebraic over F if and only if the element a is algebraic over F , but that needs to be proved.)

7. Suppose that $f(x)$ is a degree 4 polynomial with coefficients in a field F , and let K be the splitting field of $f(x)$. What are the possible values for $[K : F]$? Give examples for as many of those values as you can. (You should be able to do more than half of the possibilities; I will be impressed if you can find examples for all of them.)

Comments. None for this problem.