Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 4
February 11, 2008

Section 8.5

17. Let G be a group of order 21. We have $21 = 3 \cdot 7$. Since $7 \equiv 1 \bmod 3$, Corollary 8.18 does not apply. However, by Sylow 3, there is one Sylow 7-subgroup H, which is normal by Sylow 2. Moreover, there are either 1 or 7 Sylow 3-subgroups.

In the case that the Sylow 3-subgroup K is unique the reasoning of the proof of Corollary 8.18 applies. We have $H \cap \{e\}$ and $HK = G$ since HK contains 21 distinct elements of G. Therefore by Theorem 8.3,

$$G \simeq H \times K \simeq \mathbb{Z}_7 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{21},$$

and G is cyclic.

We now consider the case where there are 7 Sylow 3-subgroups $K_1, \ldots, K_7$. We claim that there is *only one* possible structure for G, up to isomorphism: We will show that G is generated by two elements a, b with $a^7 = e$, $b^3 = e$ and $b^{-1}ab = a^2$. Let $H = \langle a \rangle$ so $|a| = 7$. Similarly, let $K_1 = \langle b \rangle$, so $|b| = 3$. Note that since $H \cap K = \{e\}$, we have $G = \{b^j a^i : 0 \le k \le 6, 0 \le j \le 2\}$. Since H is normal, the conjugate $b^{-1}ab = a^k$ for some $k \in \{1, 2, 3, 4, 5, 6\}$. Moreover,

$$\begin{aligned} b^{-2}ab^2 &= b^{-1}(b^{-1}ab)b = b^{-1}a^k b = (b^{-1}ab)^k = (a^k)^k = a^{k^2} \\ a = b^{-3}ab^3 &= a^{k^3}, \end{aligned}$$

so

$$k^3 \equiv 1 \bmod 7. \tag{1}$$

As in the dihedral group case, knowing k in (1), or the equivalent form $ab = ba^k$ lets us determine the products

$$(b^j a^i)(b^{j'} a^{i'}) = b^{j+j'} a^{ik^{j'}+i'}.$$

This gives closure under the product operation. Associativity follows from this also since

$$\begin{aligned} \left((b^j a^i)(b^{j'} a^{i'})\right)(b^{j''} a^{i''}) &= (b^{j+j'} a^{ik^{j'}+i'})(b^{j''} a^{i''}) = b^{(j+j')+j''} a^{(ik^{j'}+i')k^{j''}+i''} \\ (b^j a^i)\left((b^{j'} a^{i'})(b^{j''} a^{i''})\right) &= (b^j a^i)(b^{j'+j''} a^{i'k^{j''}+i''}) = b^{j+(j'+j'')} a^{ik^{j'+j''}+i'k^{j''}+i''}, \end{aligned}$$

which are the same. The identity element is $e = b^0 a^0$. The inverse of $b^j a^i$ is $b^{j'} a^{i'}$ where $j' + j \equiv 0 \bmod 3$ and $ik^{j'} + i' \equiv 0 \bmod 7$. Note that $ik^{j'} + i' \equiv 0 \bmod 7$ implies that $i'k^j + i \equiv 0 \bmod 7$ also when $j' + j \equiv 0 \bmod 3$ because of (1), so this is a well-defined two-sided inverse. So we get a group of order 21 whenever the condition (1) holds.

- If $k = 1$, then G is abelian and we are back in the first case.
- We cannot have $k = 3, 5, 6$ since then $3^3 = 27 \equiv 6 \bmod 7$, $5^3 = 125 \equiv 6 \bmod 7$, and $6^3 = 216 \equiv 6 \bmod 7$.

- This leaves $k = 2, 4$. We claim these two groups are actually isomorphic. This follows since if $b^{-1}ab = a^2$, then $b^{-2}ab^2 = a^4$. The element b^2 also generates the Sylow 3-subgroup K_1, so in fact this is the same group up to isomorphism.

Section 10.2

17. (a) We have $x = \sqrt{1+\sqrt{5}}$ so $x^2 = 1 + \sqrt{5}$ and $(x^2-1)^2 = 5$, so $x^4 - 2x^2 - 4 = 0$. It is not hard to check that this polynomial is irreducible over $\mathbb{Q}$, so this is the minimal polynomial.

(b) For $x = i\sqrt{3} + \sqrt{2}$, $x^2 = -1 + 2i\sqrt{6}$, $x^3 = -3i\sqrt{3} - 7\sqrt{2}$ and $x^4 = -23 - 4i\sqrt{6}$. Hence $x^4 + 2x + 25 = 0$. It is not hard to check that this polynomial is irreducible over $\mathbb{Q}$, so this is the minimal polynomial.

19. By Theorem 10.4, we have $[F(u) : F] = [F(u) : E][E : F]$. However, by Theorem 10.7, $[F(u) : F] = p$, which is prime. Therefore either $[F(u) : E] = p$ and $[E : F] = 1$, in which case $E = F$, or $[F(u) : E] = 1$ and $[E : F] = p$, in which case $E = F(u)$.

20. We have $F \subseteq F(u^2) \subseteq F(u)$ since $u^2 \in F(u)$. Therefore, $[F(u) : F] = [F(u) : F(u^2)][F(u^2) : F]$ by Theorem 10.4. By Theorem 10.7, $[F(u) : F(u^2)]$ is either 1 or 2 since the polynomial $f(x) = x^2 - u^2$ with coefficients in $F(u^2)$ has $x = u$ as a root. But the minimal polynomial of u over F has odd degree so $[F(u) : F]$ is odd by Theorem 10.7. This implies that $[F(u) : F(u^2)] = 1$. Hence $F(u) = F(u^2)$.

23. If $u \in K$ but $u \notin \mathbb{Q}$, then have $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq K$ By Theorem 10.4 and the hypothesis $[K : \mathbb{Q}] = 2$, this implies $[\mathbb{Q}(u) : \mathbb{Q}] = 2$ and $[K : \mathbb{Q}(u)] = 1$, so $K = \mathbb{Q}(u)$. By Theorem 10.7, the minimal polynomial of u is of the form $x^2 + bx + c$ for some $b, c \in \mathbb{Q}$. Applying the quadratic formula,

$$u = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}.$$

First, we claim that $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{b^2 - 4c})$. The $\subseteq$ inclusion here is clear since $u = \frac{-b}{2} \pm \frac{1}{2}\sqrt{b^2 - 4c} \in \mathbb{Q}(\sqrt{b^2 - 4c})$. Hence $\mathbb{Q}(u) \subseteq \mathbb{Q}(\sqrt{b^2 - 4c})$. On the other hand $\sqrt{b^2 - 4c} = \mp(2u + b)$ which implies $\sqrt{b^2 - 4c} \subset \mathbb{Q}(u)$ and hence $\mathbb{Q}(\sqrt{b^2 - 4c}) \subseteq \mathbb{Q}(u)$.

Next, write $b^2 - 4c = \frac{m^2}{n^2} \cdot \frac{e}{f}$ where $m, n, e, f \in \mathbb{Z}$ are *integers* and e, f are not divisible by the square of any prime, and assume $b^2 - 4c = \frac{m^2 e}{n^2 f}$ is in lowest terms. Then $\sqrt{b^2 - 4c} = \frac{m}{n}\sqrt{\frac{e}{f}}$ and reasoning similarly to the above, we have

$$\mathbb{Q}(u) = \mathbb{Q}(\sqrt{b^2 - 4c}) = \mathbb{Q}\left(\sqrt{\frac{e}{f}}\right).$$

Finally, note that $\sqrt{\frac{e}{f}} = \frac{\sqrt{ef}}{f}$, where $f \in \mathbb{Z}$, and $d = ef$ is not divisible by the square of any prime in $\mathbb{Z}$. Then by similar reasoning to the above, we have

$$\mathbb{Q}(u) = \mathbb{Q}\left(\sqrt{\frac{e}{f}}\right) = \mathbb{Q}(\sqrt{d}),$$

which is what we wanted to show.

25. Aiming for a contradiction, suppose that u is transcendental over F, but some element of $F(u)$ not in F is algebraic over F. Then we have some

$$v = \frac{a_0 + a_1 u + \cdots + a_n u^n}{b_0 + b_1 u + \cdots + b_m u^m} \in F(u)$$

(but not in F, so $v \neq 0$) which is a root of some nonzero polynomial $f(x) = c_0 + c_1 x + \cdots + c_k x^k \in F[x]$. In the expressions for v and for $f(x)$, we may assume that $a_n \neq 0$, $b_m \neq 0$, and $c_0, c_k \neq 0$ in F. (The reason we can assume $c_0 \neq 0$ is that $v \neq 0$. So if v is a root of any polynomial in $F[x]$, then v is a root of some polynomial in $F[x]$ with nonzero constant term.) We may also assume that $f(x) = 0$ *has no roots in* F. If there are any such roots $a \in F$, then we know $f(x)$ will factor in $F[x]$ as $f(x) = (x - a)q(x)$ for some $q(x) \in F[x]$. Then $f(v) = 0$ implies $q(v) = 0$ since $v \neq a \in F$. So we can remove any factors producing roots in F and we will be left with $f(x)$ having no roots in F.

Substitute $x = v \neq 0$ in $f(x)$ and put the terms over a common denominator and collect like powers of u on the top. The result is an equation

$$0 = c_0 + c_1 v + \cdots + c_k v^k = c_0 + \cdots + c_k \left(\frac{a_0 + a_1 u + \cdots + a_n u^n}{b_0 + b_1 u + \cdots + b_m u^m} \right)^k = \frac{A_0 + A_1 u + \cdots + A_N u^N}{(b_0 + b_1 u + \cdots + b_m u^m)^k},$$

where $A_i \in F$ for all i. This implies

$$0 = A_0 + A_1 u + \cdots + A_N u^N.$$

If $n > m$ then $N = nk$ and $A_N = c_k a_n^k \neq 0$ so the polynomial $g(x) = A_0 + A_1 x + \cdots + A_N x^N$ is not zero in $F[x]$. Similarly, if $m > n$, then $N = mk$ and $A_N = c_0 b_m^k \neq 0$, so $g(x)$ is not zero in $F[x]$. Finally, if $m = n$, then $N = mk = nk$ and the coefficient A_N is

$$A_N = c_0 b_n^k + c_1 b_n^{k-1} a_n + \cdots + c_{k-1} b_n a_n^{k-1} + c_k a_n^k.$$

If $A_N = 0$, then dividing through by b_n^k we get

$$0 = c_0 + c_1 \left(\frac{a_n}{b_n} \right) + \cdots + c_k \left(\frac{a_n}{b_n} \right)^k.$$

But this implies that $f(x) = 0$ has $x = \frac{a_n}{b_n} \in F$ as a root. This contradicts what we said above about $f(x)$. Hence $A_N \neq 0$ in this case too. It follows that u is a root of a nonzero polynomial in $F[x]$, which is a contradiction to the hypothesis that u is transcendental over F.