Solution to Exam in MAT 2200, spring 2015

Exercise 1

a) Suppose $(abc)^n = e$, and that n is the smallest positive integer with this property. Then

$$(cab)^n = c(abc)^{n-1}ab = c(abc)^{-1}ab = cc^{-1}b^{-1}a^{-1}ab = e$$

By the same argument we deduce that if $(cab)^m = e$ for some positive integer $m < n$, then $(abc)^m = e$, contradicting the assumed minimality of n.

b) Let $a = (12)$, $b = (123)$ and $c = (13)$. Then $abc = (12)(123)(13) = (123)$, but $bac = (123)(12)(13) = e$.

Exercise 2 Since H is a normal subgroup of index m, G/H is a group of order m. But then $(gH)^m = (g^m)H = H$ for all $g \in G$, i.e. $g^m \in H$.

Exercise 3 By Sylow's 3rd theorem, the number of Sylow 3-subgroups is 1, 4, 7, 10, ... and the possible numbers are 1 and 7 since it should also divide 105. Similarily the number of Sylow 5-subgroups must be 1 or 21, and the number of Sylow 7-subgroups is 1 or 15. If no Sylow subgroups are normal, there will be 7 subgroups of order 3, 21 of order 5 and 15 of order 7. Except for the identity element, these groups are disjoint. Thus we have at least $7 \cdot 2 = 14$ elements of order 3, $21 \cdot 4 = 84$ elements of order 5, and $15 \cdot 6 = 90$ elements of order 7. This adds up to 188 elements in a group of order 105, which is not possible. So at least one of the Sylow subgroups has to be normal.

Exercise 4 The proof is a one-liner, using associativity:

$$b' = b' \cdot 1 = b'(ab) = (b'a)b = 1 \cdot b = b$$

Exercise 5 If $x > 0$, then $x = y^2$ for some $y \in \mathbb{R}$. It follows that $\sigma(x) = \sigma(y^2) = \sigma(y)^2 > 0$. If $a < b$, then $b - a > 0$, and $\sigma(b-a) = \sigma(b) - \sigma(a) > 0$, or $\sigma(b) > \sigma(a)$.

For any integer r we have

$$\sigma(r) = \sigma(1 + \cdots + 1) = \sigma(1) + \cdots + \sigma(1) = 1 + \cdots + 1 = r$$

since $\sigma(1) = 1$. Furthermore we have

$$m = \sigma(m) = \sigma(n \cdot \frac{m}{n}) = \sigma(n)\sigma(\frac{m}{n}) = n \cdot \sigma(\frac{m}{n})$$

(The very last statement in the exercise text follows from the fact that any real number can be written as the limit of an increasing as well as a decreasing sequence of rational numbers. By a squeezing argument σ has to fix any real number.)

EXERCISE 6 Let $f(x) = x^6 - 25$.

a)
$$x^6 - 25 = (x^3 - 5)(x^3 + 5)$$
where $x^3 \pm 5$ are irreducible by the Eisenstein criterion.

b) The roots of $f(x)$ are: α, $\omega\alpha$, $\omega^2\alpha$, $-\alpha$, $(\omega + 1)\alpha$, $(\omega^2 + 1)\alpha$, thus the splitting field is
$$K = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega)$$

c) We have $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq K = \mathbb{Q}(\alpha, \omega)$, the degree of α over $\mathbb{Q}$ is the degree of the irreducible polynom $x^3 - 5$, and
$$deg\,(\omega, \mathbb{Q}\,(\alpha)) = deg(\omega^2 + \omega + 1) = 2$$
thus
$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3$$
By looking at the very nature of the roots, we see that $G(K/\mathbb{Q}) = G(\mathbb{Q}(x^3 - 5)/\mathbb{Q})$. Let
$$\sigma : \alpha \mapsto \alpha\omega \mapsto \alpha\omega^2 \mapsto \alpha$$
(of order 3) and
$$\tau : \alpha\omega \mapsto \alpha\omega^2 \mapsto \alpha\omega, \quad \alpha \mapsto \alpha$$
(of order 2) where $\tau\sigma = \sigma^2\tau$. The only non-abelian group of order 6 is S_3.

d) We have
$$\sigma\tau(\alpha^2\omega) = \sigma\left(\tau\left(\alpha^2\omega\right)\right) = \sigma(\alpha^2\omega^2) = \alpha^2\omega^2\omega^2 = \alpha^2\omega$$
and $\mathbb{Q}(\alpha^2\omega)$ is contained in the fixed field. On the other hand we have
$$\sigma\tau(\alpha^r\omega^s) = \alpha^r\omega^r\omega^{2s} = \alpha^r\omega^{r+2s}$$
If $\alpha^r\omega^s$ is fixed then $r + 2s \equiv s$ (modulo 3), i.e. 3 divides $r + s$. Thus the non-rational fixed elements are $\alpha^2\omega$ and $\alpha\omega^2 = \frac{1}{2}(\alpha^2\omega)^2 \in \mathbb{Q}(\alpha^2\omega)$.