Qualifying Exam: Algebra

Name:..

Please give complete arguments and use good mathematical notation. Results from the notes can of course be used.

1. **(4×2 points)** True or false? Please give a proof or a counterexample (just a *true* or *false* answer, not supported by evidence, will not receive any credit).

   (a) If the finite group G has even order, then G has an index 2 subgroup.
   (b) If $K \trianglelefteq G$ and both K and G/K are abelian, then G is abelian.
   (c) Let D be a UFD. If $a, b \in D$ satisfy $\gcd(a, b) = 1$, then there are $x, y \in D$ such that $ax + by = 1$.
   (d) Let R be a commutative ring. If $R[x]$ is a UFD, then R is a PID.

2. **(5 points)** Let $p \geq 2$ be a prime and $n \geq 1$. Show that every group of order $2p^n$ is solvable. *Suggestion:* Use Theorem 3.36.

3. **(4 points)** Assume that $K \trianglelefteq G$ and $K \cap G' = 1$ (where G' denotes the commutator subgroup of G). Show that K is contained in the center of G.

4. **(4×3 points)** Consider the group

$$G = \langle a, b | a^6 = 1, b^2 = a^3, ba = a^{-1}b \rangle.$$

   (a) Show that G has at most 12 elements. *Suggestion:* Use the third relation to move a's to the left in a given word.
   (b) Show that G is isomorphic to the subgroup $\langle A, B \rangle \subseteq (\mathbb{H}^\times, \cdot)$ of the quaternions that is generated by

$$A = \begin{pmatrix} e^{i\pi/3} & 0 \\ 0 & e^{-i\pi/3} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

   (or, if you prefer, just view this as a subgroup of $SL(2, \mathbb{C})$). Then deduce that G has *exactly* 12 elements. *Suggestion:* Use Dyck's theorem.
   (c) Show that G is not abelian and not isomorphic to the dihedral group D_6. *Suggestion:* Look for elements of order 2.
   (d) Find the center C of G and identify G/C (what familiar group is this quotient isomorphic to?). *Remark:* This second part could be done by hand, of course, but it would be more convenient to make use of some theoretical results.

5. **(2+2+3+2 points)** Consider the domain $D = \mathbb{Z}[\sqrt{-3}]$.

   (a) What are the units of D? *Suggestion:* In this and the subsequent parts of this problem, the *norm* $N(x) = a^2 + 3b^2 = |x|^2$, $x = a + b\sqrt{-3} \in D$ should be a useful tool.
   (b) Show that D satisfies the DCC.
   (c) Factor $x = 4$ into irreducible elements in two different ways (don't forget to prove that your factors are in fact irreducible, and that they are not associates).
   (d) Find an irreducible element that is not a prime.

6. **(3+3+3 points)** (a) Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 3. Show that the Galois group of f is isomorphic to $\mathbb{Z}_3$ or S_3.
(b) Find an irreducible polynomial $f \in \mathbb{Q}[x]$ with Galois group isomorphic to $\mathbb{Z}_6$. *Suggestion:* Use Theorem 6.31.
(c) Suppose that the Galois group of $f \in \mathbb{Q}[x]$ has odd order. Prove that then all (complex) zeros of f are real.

7. **(2+2+2+4 points)** Consider $f = x^p - x - a \in \mathbb{Z}_p[x]$, with $a \in \mathbb{Z}_p$, $a \neq 0$.

   (a) Show that f has no zeros in $\mathbb{Z}_p$.
   (b) Show that f is separable.
   (c) Let $F/\mathbb{Z}_p$ be a field extension, and suppose that $b \in F$ satisfies $f(b) = 0$. Prove that then also $f(b+1) = 0$.
   (d) Deduce from parts (a), (c) that $E = \mathbb{Z}_p(b)$ is a splitting field for any such b and F, the Galois group $\mathrm{Gal}(E/\mathbb{Z}_p)$ is cyclic of order p, and f is irreducible over $\mathbb{Z}_p$.

8. **(2+2+3+4 points)** Let $a = \sqrt{5} - \sqrt{2}$.

   (a) Show that $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ (and we define these as subfields of $\mathbb{C}$).
   (b) Show that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.
   (c) Find the minimal polynomial $f_a \in \mathbb{Q}[x]$ of a over $\mathbb{Q}$; please don't forget to explain why the polynomial you propose is irreducible.
   (d) Prove that $\mathbb{Q}(a)/\mathbb{Q}$ is Galois, and find the Galois group: more precisely, describe the automorphisms, and also find a familiar group that $\mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q})$ is isomorphic to.