1a) Determine the units of $\mathbb{Z}_4$ and $\mathbb{Z}_{12}$ and write down Cayley tables for the multiplicative groups $U(\mathbb{Z}_4)$ and $U(\mathbb{Z}_{12})$ of these units. (The congruence classes should be represented by the smallest positive integers in the tables.)

b) Decide if $U(\mathbb{Z}_4)$ and $U(\mathbb{Z}_{12})$ are isomorphic or not.

2. Prove or disprove that every abelian group of order 2013 is cyclic.
   (Hint: $2013 = 11 \times 183$.)

3. Prove that $5 + 12i$ is reducible in the ring $\mathbb{Z}[i]$ of Gaussian integers.
   (Hint: Use the norm map from $\mathbb{Z}[i]$ to $\mathbb{Z}$ to find a factorisation.)

4a) Prove that $f(x) = (x^3 + x + 1)^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

b) Let $K$ be the quotient ring $\mathbb{Z}_2[x]/I$ of the principal ideal $I = (f(x))$ in $\mathbb{Z}_2[x]$.
   Explain why the set of non-zero elements in $K$ form a multiplicative group $G$ and determine the order of this group.

c) Determine the order of the element $(x^3 + x + 1)(x + 1) + I$ in $G$.

5. Let $G$ be a group and $a \in G$ be an element such $a^r = a^s$ for two different integers $r$ and $s$. Show the following statements.

a) There is a smallest positive integer with $a^n = e$.

b) If $i$ is an integer, then $a^i = e$ if and only if $n$ is a divisor of $i$.

c) The elements $e = a^0, a, a^2, \ldots, a^{n-1}$ are distinct and represent all elements in the cyclic subgroup generated by $a$.

6. Let $K$ be a field. Prove that any ideal of $K[x]$ is a principal ideal.

*The theorems in Durbin's book may be used to solve the exercises 1-4, but all claims that are made must be motivated. The exam will be corrected within three weeks.*
Solutions to the examination in algebra MMG 500 and MVE 150, 2013-03-15

1a) The units in $\mathbb{Z}_n$ are given by $[k]_n$ for positive integers $k \leq n$ relatively prime to $n$. If we write $k$ instead of $[k]_n$, then the Cayley tables for $\mathbb{Z}_6$ resp. $\mathbb{Z}_{12}$ are given by

\[
\begin{array}{cccccc}
\times & 1 & 3 & 5 & 7 & 11 \\
1 & 1 & 3 & 5 & 7 & 11 \\
3 & 3 & 1 & 7 & 5 & 11 \\
5 & 5 & 7 & 1 & 3 & 11 \\
7 & 7 & 5 & 3 & 1 & 11 \\
\end{array}
\]

b) $U(\mathbb{Z}_6)$ and $U(\mathbb{Z}_{12})$ are both abelian of order 4 with all elements $\neq 1$ of order two. They are therefore both isomorphic to the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$ by the fundamental theorem for finite abelian groups and hence isomorphic to each other.

2. $2013 = 3 \times 11 \times 61$ where 3, 11 and 61 are primes. Any abelian group $A$ of order 2013 is therefore isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{61}$ by the fundamental theorem for finite abelian groups. In particular, we have that $\mathbb{Z}_{2013} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{61}$ and by transitivity that $A \cong \mathbb{Z}_{2013}$. Every abelian group of order 2013 is thus cyclic.

3. Let $a+bi$ be a Gaussian integer, which divides $5+12i$. Then by the multiplicativity of the norm $N(a+bi) = a^2 + b^2$, we get that $a^2 + b^2$ divides $5^2 + 12^2 = 169$. Hence $a^2 + b^2 = 1, 13$ or $12^2$, where $a^2 + b^2 = 1$ and $13^2$ lead to factorizations of $5+12i$ where one of the factors is a unit.

We are thus led to study factors $a+bi$ with $a^2 + b^2 = 13$. But then $(a, b) = (\pm 2, \pm 3)$ or $(\pm 3, \pm 2)$ and is now easy to verify that $(2-3i)(2+3i) = (3+2i)(-3-2i) = 5+12i$.

4a) There was a misprint in the exam. We assume here that $f(x) = (x^2 + x + 1)^2 + (x+1)x$. Then, $f(x)$ has no linear factor in $\mathbb{Z}_2[x]$ by the factor theorem as $f(0) = f(1) = 1$. If $f(x)$ were reducible in $\mathbb{Z}_2[x]$, it would thus have a monic quadratic irreducible factor. But $x^2$, $x^2 + x + (x+1)x$ and $x^2 + 1 = (x+1)^2$ are all reducible in $\mathbb{Z}_2[x]$. If $f(x)$ were reducible, it would thus have $x^2 + x + 1$ as a factor. But this is not the case as $f(x) = (x^2 + x + 1)^2 + (x^2 + x + 1) + 1$. So $f(x)$ must be irreducible.

b) By a theorem in Durbin’s book we have that $K = \mathbb{Z}_2[x]/(f(x))$ is a field as $f(x)$ is irreducible. The set $G$ of non-zero elements in the field $K$ form thus a multiplicative group. By the division algorithm for $\mathbb{Z}_2[x]$ any element in $K = \mathbb{Z}_2[x]/(f(x))$ is uniquely represented by a polynomial $a_0 + a_1x + a_2x^2 + ax^3 \in \mathbb{Z}_2[x]$. There are thus $2^4$ elements in $K$ such that $G$ is of order $2^4 = 16$.

c) Let $g = (x^2 + x + 1)(x+1) + I$, $a = (x+1) + I$ and $b = x + I$. Then $g^2 = (x^2 + x + 1)^2(x+1)^2 + I = a^2b$ since $(x^2 + x + 1)^2 + I = (x+1)x + I$. Moreover, $a \neq e$, $a \neq e$, $b \neq e$ and $b \neq e$ as $(x+1)^2 + I = x(x^2 + x + 1)$.
\((x+1)^3-1, x^2-1=(x-1)(x^2+x^2+x+1)\) and \(x^2-1\) are not divisible by \(f(x)\) in \(\mathbb{Z}_p[x]\). Hence, \(o(a)\) \n 15 as the order of an element in \(G\) divides \(|G|\). There is therefore some \(k\) with \(GCD(k, 15)=1\) such that \(b=a^k\) and \(e \neq g^2 = a^{3k}\). But then \(o(g) = o(g^2) = o(a)GCD(k+3, 15)=3\) or 15. Finally, \(o(g) \neq 3\) since \(g^2 = g \cdot g = a^3 \cdot g = (x+1)^4(x^2+x+1) = 1\) is not divisible by \(f(x)\) in \(\mathbb{Z}_p[x]\). Hence \(o(g) = 15\).

5. See Durbin's book

6. See Durbin's book