MATHEMATICS Chalmers University of Technology
Examination in algebra MMG 500 and MVE 150, 2013-03-15
No books, written notes or any other aids are allowed.
Telephone : 0762-721860 or 0762-721861 / 0703-088304

1a) Determine the units of $\mathbf{Z}_8$ and $\mathbf{Z}_{12}$ and write down Cayley tables for the multiplicative groups $U(\mathbf{Z}_8)$ and $U(\mathbf{Z}_{12})$ of these units. (The congruence classes should be represented by the smallest positive integers in the tables.) 3p

b) Decide if $U(\mathbf{Z}_8)$ and $U(\mathbf{Z}_{12})$ are isomorphic or not. 2p

2. Prove or disprove that every abelian group of order 2013 is cyclic. 3p
(Hint : $2013 = 11\times 183$.)

3. Prove that $5+12i$ is reducible in the ring $\mathbf{Z}[i]$ of Gaussian integers. 4p
(Hint : Use the norm map from $\mathbf{Z}[i]$ to $\mathbf{Z}$ to find a factorisation.)

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

b) Let K be the quotient ring $\mathbf{Z}_2[x]/I$ of the principal ideal $I=(f(x))$ in $\mathbf{Z}_2[x]$. Explain why the set of non-zero elements in K form a multiplicative group G and determine the order of this group. 2p

c) Determine the order of the element $(x^2+x+1)(x+1)+I$ in G. 2p

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. 4p

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

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

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. 3p

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 $\mathbf{Z}_n$ are given by $[k]_n$ for positive integers $k \le n$ relatively prime to n. If we write k instead of $[k]_n$, then the Cayley tables for $\mathbf{Z}_8$ resp. $\mathbf{Z}_{12}$ are given by

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

b) $U(\mathbf{Z}_8)$ and $U(\mathbf{Z}_{12})$ are both abelian of order 4 with all elements$\neq 1$ of order two. They are therefore both isomorphic to the *additive* group $\mathbf{Z}_2 \times \mathbf{Z}_2$ 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 thence isomorphic to $\mathbf{Z}_3 \times \mathbf{Z}_{11} \times \mathbf{Z}_{61}$ by the fundamental fundamental theorem for finite abelian groups. In particular, we have that $\mathbf{Z}_{2013} \cong \mathbf{Z}_3 \times \mathbf{Z}_{11} \times \mathbf{Z}_{61}$ and by transitivity that $A \cong \mathbf{Z}_{2013}$. 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 $5^2+12^2=13^2$. Hence $a^2+b^2=1, 13$ or 13^2, 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 $(2-3i)(-2+3i) = (3+2i)^2 = (-3-2i)^2 = 5+12i$.

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 $\mathbf{Z}_2[x]$ by the factor theorem as $f(0)=f(1)=1$. If $f(x)$ were reducible in $\mathbf{Z}_2[x]$, it would thus have a monic quadratic irrreducible factor. But x^2, $x^2+x=(x+1)x$ and $x^2+1=(x+1)^2$ are all reducible in $\mathbf{Z}_2[x]$. If $f(x)$ were reducible, it would thus have x^2+x+1 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 $K=\mathbf{Z}_2[x]/(f(x))$ 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 $\mathbf{Z}_2[x]$ any element in $K=\mathbf{Z}_2[x]/(f(x))$ is uniquely represented by a polynomial $a_0+a_1x+a_2x^2+a_3x^3 \in \mathbf{Z}_2[x]$. There are thus 2^4 elements in K such that G is of order $2^4-1=15$.

c) Let $g=(x^2+x+1)(x+1)+I$, $a=(x+1)+I$ and $b=x+I$. Then $g^2=(x^2+x+1)^2(x+1)^2+I=a^3b$ since $(x^2+x+1)^2+I=(x+1)x+I$. Moreover, $a^5 \neq e$, $a^3 \neq e$, $b^5 \neq e$ and $b^3 \neq e$ as $(x+1)^5-1=x(x^4+x^3+1)$,

$(x+1)^3-1$, $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$ and x^3-1 are not divisible by $f(x)$ in $\mathbf{Z}_2[x]$. Hence, $o(a)=$ $o(b)=15$ as the order of an element in G divide $|G|=15$. There is therefore some k with GCD(k, 15)=1 such that $b=a^k$ and $e\neq g^2=a^{k+3}$. But then $o(g)=o(g^2)=o(a)/$ GCD(k+3, 15)= 3 or 15. Finally, $o(g)\neq 3$ since $g^3=g^2g=a^3b\,g=(x+1)^4x(x^2+x+1)-1$ is not divisible by $f(x)$ in $\mathbf{Z}_2[x]$. Hence $o(g)=15$.

5. See Durbin's book

6. See Durbin's book