SF2729 GROUPS AND RINGS
Final Exam
Friday June 1, 2012

Time: 14:00–18:00
Allowed aids: none
Examiners: Wojciech Chachólski and Carel Faber

Present your solutions to the problems in such a way that the arguments and calculations are easy to follow. Provide detailed arguments to your answers. An answer without explanation will be given no points.

For Problem 1, the final score equals at least the number of points obtained from the homeworks of the groups part of the course. If your solution to Problem 1 is worth more points, then this will be your final score.

For Problem 2, the final score equals at least the number of points obtained from the homeworks of the rings part of the course. If your solution to Problem 2 is worth more points, then this will be your final score.

For each problem, the maximum score is 6 points.

The minimum requirements for the various grades are according to the following table:

Grade	**A**	**B**	**C**	**D**	**E**
Total credit	30	27	24	21	18

Problem 1

(6 points). List all groups of order 6 up to isomorphism and prove that these are all such groups.

Solution

Let G be a group of order 6. Since the primes 2 and 3 divide the number 6, there are elements a and b in G whose orders are respectively 2 and 3. The subgroup $< b >$ has 3 elements $(1, b, b^2)$, hence has index 2 and therefore is normal in G.

There are two possibilities. One is when a and b commute with each other. In this case the group $< a, b >$ is abelian and since $< a > \cap < b >= \{1\}$, it has 6 elements. It follows that G is abelian and therefore is isomorphic to $\mathbf{Z}/6$.

Assume now that a and b do not commute. Note that the following elements in G are all different: $1, b, b^2, a, ab, ab^2$. Since $< b >= \{1, b, b^2\}$ is normal in G the conjugation with respect to any element of G maps the set $\{1, b, b^2\}$ onto itself. This defines a function $f : G \to S_{\{1,b,b^2\}}$, that maps an element g to the permutation of $\{1, b, b^2\}$ given by the conjugation $g - g^{-1}$ with g. This is a group homomorphism. We are going to check that its kernel consists only of 1. For that we need to show that for any $g \neq 1$, $f(g)$ is not the identity permutation of $\{1, b, b^2\}$.

- $f(a)(b) = aba$ can not be equal to b since $aba = b$ implies commutativity $ab = ba$. It follows that $aba = b^2$.

- $f(b)(a) = bab^2$ can not be equal to a since the equality $bab^2 = a$ implies $abab^2 = 1$, which by the previous argument would lead to a contradiction $b = b^4 = 1$.
- $f(ab)(a) = abab^2a = b^4a = ba = aaba = ab^2$ is not equal to a.
- $f(ab^2)(a) = ab^2aba = ab^4 = ab$ is not equal to a.
- $f(b^2)(a) = b^2ab$ can not be equal to a since the equality $b^2ab = a$ implies $b^2aba = 1$ which leads to a contradiction $b^4 = b = 1$.

We have constructed an isomorphism between G and $S_{\{1,b,b^2\}}$.

Conclusion: up to an isomorphism there are only 2 groups of order 6, the cyclic group $\mathbf{Z}/6$ and the permutation group S_3.

Problem 2

Let R be the ring

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \,|\, a, b \in \mathbb{Z}\}.$$

It is given that R is a Euclidean domain with Euclidean multiplicative norm

$$N(a + b\sqrt{-2}) = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2.$$

a. **(2 points)**. Prove that $1 + 2\sqrt{-2}$ is not an irreducible element of R.

b. **(2 points)**. Determine a greatest common divisor in R of $2 + \sqrt{-2}$ and $4 + \sqrt{-2}$.

c. **(2 points)**. Prove that $R/\langle 3 + \sqrt{-2}\rangle$ is a finite field with 11 elements.

Solution

a. The norm of $1 + 2\sqrt{-2}$ equals 9. If $1 + 2\sqrt{-2} = x \cdot y$ with x and y non-units in R, then x and y must have norm 3, since the norm is multiplicative. (Note that a unit must have norm 1; conversely, the only elements with norm 1 are 1 and -1, which are units.) The only elements with norm 3 are $\pm 1 \pm \sqrt{-2}$. Now $(1 + \sqrt{-2})(1 - \sqrt{-2}) = 3$, so the only possible factorizations (up to units) of $1 + 2\sqrt{-2}$ are $\pm(1 \pm \sqrt{-2})^2$. We see that $(1+\sqrt{-2})^2 = -1+2\sqrt{-2}$, which doesn't help us, but $-(1-\sqrt{-2})^2 = -(-1-2\sqrt{-2}) = 1 + 2\sqrt{-2}$, which proves that $1 + 2\sqrt{-2}$ is not irreducible in R.

b. A fast way of solving this is to observe that the difference of $4+\sqrt{-2}$ and $2+\sqrt{-2}$ equals 2, that the difference of $2 + \sqrt{-2}$ and 2 equals $\sqrt{-2}$, and that $\sqrt{-2}$ clearly divides both $4 + \sqrt{-2}$ and $2 + \sqrt{-2}$ (since it divides 2). Thus $\sqrt{-2}$ is a greatest common divisor in R of $2 + \sqrt{-2}$ and $4 + \sqrt{-2}$.

   More precisely, above we have applied the Euclidean algorithm to find a g.c.d. of $4+\sqrt{-2}$ and $2 + \sqrt{-2}$. The norm of $4 + \sqrt{-2}$ is 18, that of $2 + \sqrt{-2}$ is 6, and that of 2 is 4, so 2 is a remainder when $4 + \sqrt{-2}$ is divided by $2 + \sqrt{-2}$. Similarly, $\sqrt{-2}$, with norm 2, is a

remainder when $2+\sqrt{-2}$ is divided by 2. Finally, dividing 2 by $\sqrt{-2}$, the remainder is 0, so $\sqrt{-2}$ is a g.c.d. of $4+\sqrt{-2}$ and $2+\sqrt{-2}$.

c. A Euclidean domain is a PID, and nonzero ideals in a PID are maximal if and only if they are generated by an irreducible element. The norm of $3+\sqrt{-2}$ equals 11, a prime number. It directly follows that $3+\sqrt{-2}$ is irreducible (the norm is multiplicative). So $\langle 3+\sqrt{-2}\rangle$ is a maximal ideal and therefore $R/\langle 3+\sqrt{-2}\rangle$ is a field F. Moreover, by the definition of the norm, $\langle 3+\sqrt{-2}\rangle$ contains 11, so that $11=0$ in F, which implies that F has characteristic 11. Since $\sqrt{-2}=-3$ in F, we see that F consists of the 11 elements $\overline{a}$, where $0\leq a\leq 10$.

Problem 3

a. **(2 points)**. Let H be a subgroup of a group G. Show that if $(G:H)=2$, then H is a normal subgroup of G.

b. **(1 point)**. Find an example of a group G and a subgroup H for which $(G:H)=3$ and H is a normal subgroup of G.

c. **(3 points)**. Find an example of a group G and a subgroup H for which $(G:H)=4$ and H is NOT a normal subgroup of G.

Solution

a. Consider a left coset aH. If $aH=H$, then a is in H and hence $aH=Ha$. If $aH\neq H$, then a does not belong to H and consequently the right coset Ha is not equal to H. It follows that $\{H,Ha\}$ are the two different right cosets of H in G. Since the index of H in G is 2, the group G is the disjoint union of H and aH. Similarly G is the disjoint union of H and Ha. It follows that $aH=Ha$.

   We can conclude that for any a, $aH=Ha$. This means that H is a normal subgroup in G.

b. For example take $G=\mathbf{Z}/6$ and $H=<2>$.

c. For example take $G=S_{\{1,2,3,4\}}$ and $H=S_{\{1,2,3\}}=\{\sigma\in S_{\{1,2,3,4\}}\mid \sigma(4)=4\}$. The order of H is 6 and the order of G is 24. Thus the index of H in G is 4. The cycle $(1,2,3)$ belongs to H, however its conjugation $(3,4)(1,2,3)(3,4)=(1,2,4)$ does not. It follows that H is not normal in G.

Problem 4

a. **(2 points)**. Show that x^2+x+1 is the only irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$.

b. **(2 points)**. Show that a polynomial of degree 5 in $\mathbb{Z}_2[x]$ which has no zeroes in $\mathbb{Z}_2$ and which is not divisible by x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$.

c. **(2 points)**. Show that $x^5 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$ and determine a generator for the multiplicative group of $\mathbb{Z}_2[x]/\langle x^5 + x^2 + 1\rangle$.

Solution

a. There are only 4 polynomials of degree 2 in $\mathbb{Z}_2[x]$: x^2, $x^2 + 1$, $x^2 + x$, and $x^2 + x + 1$. The polynomials with constant term 0 are divisible by x. Of course $x^2 + 1 = (x + 1)^2$ in $\mathbb{Z}_2[x]$. On the other hand, $x^2 + x + 1$ is a polynomial of degree 2 without zeroes in $\mathbb{Z}_2$, so it is irreducible in $\mathbb{Z}_2[x]$.

b. Consider a polynomial of degree 5 in $\mathbb{Z}_2[x]$ which has no zeroes in $\mathbb{Z}_2$. The only factorization it can have is as a polynomial of degree 2 times a polynomial of degree 3, both irreducible. But by (a) above, $x^2 + x + 1$ is the only irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$, and the given polynomial is not divisible by $x^2 + x + 1$. Therefore, it is irreducible.

c. We apply (b) above. Note that $x^3+1 = x^3-1 = (x-1)(x^2+x+1) = (x+1)(x^2+x+1)$, so $x^5 + x^2 + 1 = x^2(x + 1)(x^2 + x + 1) + 1$, so $x^5 + x^2 + 1$ is not divisible by $x^2 + x + 1$. Clearly, it has no zeroes either, so it is irreducible in $\mathbb{Z}_2[x]$. We know that this means that it generates a maximal ideal in $\mathbb{Z}_2[x]$, so the quotient $\mathbb{Z}_2[x]/\langle x^5 + x^2 + 1\rangle$ is a field, which is easily seen to have $2^5 = 32$ elements. Its multiplicative group has 31 elements, a prime number. Hence any element not equal to the identity element 1 is a generator; perhaps it is most natural to take $\overline{x} = x + \langle x^5 + x^2 + 1\rangle$.

Problem 5

Let S_{12} be the permutation group of the set $\{1, 2, 3, \ldots, 12\}$.

a. **(1 point)**. Is there an element τ in S_{12} for which τ^2 is odd?

b. **(2 points)**. Consider the following permutation in S_{12}:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 1 & 12 & 11 & 7 & 10 & 9 & 6 & 8 & 4 & 5 \end{pmatrix}$$

Find the cycle decomposition of σ and of σ^2. Determine if σ is odd or even.

c. **(3 points)**. Find the maximal order of a cyclic subgroup of S_{12}.

Solution

a. Write τ as a product of transpositions $\tau = t_1 t_2 \cdots t_k$. It follows that $\tau^2 = t_1 \cdots t_k t_1 \cdots t_k$ is a product of an even number of transpositions and hence it is even. We can conclude that there is no τ for which τ^2 is odd.

b. $\sigma = (1,2,3)(4,12,5,11)(6,7,10,8,9)$ and $\sigma^2 = (1,3,2)(4,5)(12,11)(6,10,9,7,8)$.

We can therefore write σ as the following product of an odd number of transpositions:

$$\sigma = (1,3)(1,2)(4,11)(4,5)(4,12)(6,9)(6,8)(6,10)(6,7)$$

Thus the permutation σ is odd.

c. Let τ be a permutation in S_n. Express τ as a product $c_1 c_2 \cdots c_k$ of disjoint cycles. Let $|c_i|$ denote the length of the cycle c_i. This number is the order of the cyclic subgroup $< c_i >$ in S_n. Since the cycles c_1, c_2, ..., c_k commute with each other, as they are disjoint, the subgroup $< c_1, c_2, \ldots, c_k >$ is isomorphic to $\mathbf{Z}/|c_1| \times \mathbf{Z}/|c_2| \times \cdots \times \mathbf{Z}/|c_k|$. The element $(1,1,\ldots,1)$ in this abelian group has order equal to the least common multiple of the numbers $|c_1|$, $|c_2|$,..., $|c_k|$. We can conclude that this least common multiple is the order of the permutation τ.

For example the element σ from part (b) has order equal to the least common multiple of $\{3,4,5\}$ which is 60. We claim that this is the maximal order of a cyclic subgroup in S_{12}. Let τ be an arbitrary permutation in S_{12}. Write it as a disjoint product of cycles $\tau = c_1 c_2 \cdots c_k$. We call the sequence of numbers $[|c_1|, |c_2|, \ldots, |c_k|]$ the cycle type of τ.

- If one of the cycles has order 12 or 11, then the cycle type of τ can be either $[12]$ or $[11]$, Thus τ has order 12 or 11.
- If one of the cycles has order 10, then the cycle type of τ can be either $[10]$ or $[10,2]$. Consequently τ has order 10.
- If one of the cycles has order 9, then the cycle type of τ can be either $[9]$ or $[9,2]$ or $[9,3]$. Consequently the order of τ can be either 18 or 9.
- If one of the cycles has order 8, then the cycle type of τ can be either $[8]$ or $[8,2]$, or $[8,2,2]$ or $[8,3]$, or $[8,4]$. In this case the order of τ is either 8 or 24.
- If one of the cycles has order 7, then the cycle type of τ can be either $[7]$, or $[7,2]$, or $[7,3]$, or $[7,4]$ or $[7,5]$, or $[7,2,2]$, or $[7,2,3]$. In this case the order of τ is either 7, 14, 21, 28, 35, or 42.
- If one of the cycles has order 6, then the cycle type of τ can be either $[6]$, or $[6,2]$, or $[6,3]$, or $[6,4]$, or $[6,5]$, or $[6,6]$, or $[6,2,2]$, or $[6,2,3]$, or $[6,2,4]$, or $[6,3,3]$. In this case the order of τ is either 6, 12, or 30.
- If one of the cycles has order 5, then the cycle type of τ can be either $[5]$, or $[5,2]$, or $[5,3]$, or $[5,4]$, or $[5,5]$, or $[5,6]$, or $[5,7]$, or $[5,2,2]$, or $[5,2,3]$, or $[5,2,4]$, or $[5,2,5]$, or $[5,3,3]$, or $[5,3,4]$. In this case the order of τ is either 5, 10, 15, 20, 30, 35, or 60.
- If all the cycles are of length not bigger than 4, then the order of τ can not be bigger than 12.

Problem 6

Let A be the set of complex numbers that are algebraic over $\mathbb{Q}$.

a. **(3 points)**. Prove that A is a subfield of $\mathbb{C}$.

b. **(3 points)**. Prove that A is algebraically closed.

Solution

a. Let α and β be in A. We need to show that $\alpha + \beta$ and $\alpha\beta$ are in A and that $1/\alpha$ is in A if $\alpha \neq 0$. We know that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are finite over $\mathbb{Q}$, and clearly $\mathbb{Q}(\alpha)(\beta)$ is finite over $\mathbb{Q}(\alpha)$. So $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)(\beta)$ is finite over $\mathbb{Q}$, and every element of it belongs therefore to A. But $\mathbb{Q}(\alpha, \beta)$ is the smallest field extension of $\mathbb{Q}$ containing α and β, so it contains $\alpha + \beta$ and $\alpha\beta$, and $1/\alpha$ if $\alpha \neq 0$.

b. Let $f(x) \in A[x]$ be a nonconstant polynomial. We need to show that $f(x)$ has a zero in A. Certainly, $f(x)$ has a zero α in $\mathbb{C}$, since $\mathbb{C}$ is algebraically closed. Write $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 1$, $a_n, \ldots, a_0$ in A, and $a_n \neq 0$. Repeating the arguments in (a), we see that $\mathbb{Q}(a_n, \ldots, a_0)$ is finite over $\mathbb{Q}$, and $\mathbb{Q}(a_n, \ldots, a_0)(\alpha)$ is finite over $\mathbb{Q}(a_n, \ldots, a_0)$, so $\mathbb{Q}(a_n, \ldots, a_0, \alpha)$ is finite over $\mathbb{Q}$, so $\alpha \in A$, and $f(x)$ has a zero in A. (Of course it follows that $f(x)$ factors in $A[x]$ into linear factors.)