Solution sketches for Exam 2

1. (a) Write the permutation $\sigma = \left( \begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
5 & 6 & 7 & 2 & 3 & 4
\end{array} \right)$ in cycle form.

(b) Write $\sigma$ as a product of transpositions.

(c) Decide if $\sigma$ is an even or an odd permutation.

Solution: (a) $\sigma = (1 \ 5 \ 3 \ 7)(2 \ 6 \ 4)$.

(b) $\sigma = (1 \ 7)(1 \ 3)(1 \ 5)(2 \ 4)(2 \ 6)$.

(c) As a product of an odd number of transpositions $\sigma$ must be odd.

2. Let $\alpha = (2 \ 5 \ 3)(1 \ 4 \ 6)$ and $\beta = (1 \ 6 \ 2)(5 \ 3 \ 7 \ 4)$.

Determine the order of $\alpha$ and $\beta$. Compute $\alpha \beta$, $\beta^4$ and $\alpha^{-1}$. Give the answer in cycle form.

Solution: The order of $\alpha$ is $\text{l.c.m.}(3, 3) = 3$, the order of $\beta$ is $\text{l.c.m.}(3, 4) = 12$.

Without calculation one sees $\beta^4 = (1 \ 6 \ 2)$ and $\alpha^{-1} = (2 \ 3 \ 5)(1 \ 6 \ 4)$. The computation of $\alpha \beta$ is left to the reader.

3. (Ring Sudoku) Suppose that $R = \{x, y, z, w\}$ is a ring. Complete the multiplication table below.

<table>
<thead>
<tr>
<th>+</th>
<th>$x$</th>
<th>$y$</th>
<th>$z$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
<td>$w$</td>
</tr>
<tr>
<td>$y$</td>
<td>$y$</td>
<td>$z$</td>
<td>$w$</td>
<td>$x$</td>
</tr>
<tr>
<td>$z$</td>
<td>$z$</td>
<td>$w$</td>
<td>$x$</td>
<td>$y$</td>
</tr>
<tr>
<td>$w$</td>
<td>$w$</td>
<td>$x$</td>
<td>$y$</td>
<td>$z$</td>
</tr>
</tbody>
</table>

Solution: Note that $(R, +)$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +)$ with (possible) generator $y$ ($x = 0y$, $y = 1y$, $z = 2y$, $w = 3y$, where $my$ stands for the sum of $m$ copies of $y$). By the distributivity law one has $(my) \cdot (ny) = (mn)(y \cdot y)$ which together with $y \cdot y = z = 2y$ gives

<table>
<thead>
<tr>
<th>$\cdot$</th>
<th>$x$</th>
<th>$y$</th>
<th>$z$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$x$</td>
<td>$x$</td>
<td>$x$</td>
<td>$x$</td>
</tr>
<tr>
<td>$y$</td>
<td>$x$</td>
<td>$z$</td>
<td>$x$</td>
<td>$z$</td>
</tr>
<tr>
<td>$z$</td>
<td>$x$</td>
<td>$x$</td>
<td>$x$</td>
<td>$x$</td>
</tr>
<tr>
<td>$w$</td>
<td>$x$</td>
<td>$z$</td>
<td>$x$</td>
<td>$z$</td>
</tr>
</tbody>
</table>
4. Consider the subsets $\mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbb{Z}\}$ and $\mathbb{Q}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ of the real numbers $\mathbb{R}$.

(a) Show that $\mathbb{Z}[\sqrt{2}]$ is an integral domain but not a field with respect to the addition and multiplication of $\mathbb{R}$.

(b) Show that $\mathbb{Q}[\sqrt{2}]$ is a field with respect to the addition and multiplication of $\mathbb{R}$.

**Solution:** Since the real numbers $\mathbb{R}$ form a ring, the subsets $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}]$ form rings if they are closed under the addition and multiplication which is directly checked. They are also both integral domains since $\mathbb{R}$ as a field is an integral domain. (Alternatively: a nontrivial solution of $(x+\sqrt{2}y)(a+\sqrt{2}b) = 0$ gives for $xb + ya \neq 0$ the equation $\sqrt{2} = -\frac{xa + 2yb}{xb + ya}$, a contradiction to the irrationality of $\sqrt{2}$. If $xb + ya = 0$ it follows that $xa + 2yb = 0$. Since the determinant of this linear system seen as an equation for $x$ and $y$ is $2b^2 - a^2$, the only solution is $x = y = 0$ if $2b^2 - a^2 \neq 0$. If $2b^2 - a^2 = 0$, the irrationality of $\sqrt{2}$ implies $a = b = 0$. Thus either $x + \sqrt{2}y$ or $a + \sqrt{2}b$ is zero.) The ring $\mathbb{Z}[\sqrt{2}]$ is not a field since $(x + \sqrt{2}y)(1/\sqrt{2}) = 1$ gives for $x \neq 0$ the solution $\sqrt{2} = \frac{1-2y}{x}$ which is impossible by the irrationality of $\sqrt{2}$. Thus $x = 0$ and $y = 1/2$ which is not integral. Therefore, $\sqrt{2}$ has no inverse in $\mathbb{Z}[\sqrt{2}]$. The ring $\mathbb{Q}[\sqrt{2}]$ is a field since $\frac{1}{x+\sqrt{2}y} = \frac{x-\sqrt{2}y}{x^2-2y^2} \in \mathbb{Q}[\sqrt{2}]$ for $x^2 - 2y^2 \neq 0$, but $x^2 - 2y^2 = 0$ implies $\sqrt{2} = y/x$ for $y \neq 0$ which is impossible or $y = 0$ and $x = 0$ which gives $x + \sqrt{2}y = 0$.

5. If $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an ascending chain of ideals of a ring $R$, prove that $I = \bigcup_{n=1}^{\infty} I_n$ (i.e. the union of all the ideals $I_n$) is an ideal of $R$.

**Solution:** Let $a, b \in I$ and $r \in R$. Then $a \in I_n$ and $b \in I_m$ for some $m$ and $n$. This implies $a, b \in I_k$, where $k$ is the maximum of $m$ and $n$ since $I_m \subset I_k$ and $I_n \subset I_k$. Because $I_k$ is an ideal one has $a + b$, $-a$, $ra$, $ar \in I_k$. Thus $a + b$, $-a$, $ra$, $ar \in I$ since $I_k \subset I$. This implies that $I$ is an ideal.

6. Consider the two ideals $I = (225) = 225\mathbb{Z}$ and $J = (30) = 30\mathbb{Z}$ in the ring of integers. Determine the ideals

(a) $I + J := \{i + j \mid i \in I, j \in J\}$,

(b) $I \cap J := \{x \mid x \in I, x \in J\}$,

(c) $IJ := \{x \mid x$ is sum of elements of the form $ij$ with $i \in I, j \in J\}$.

**Solution:** (a) $I + J$ is generated by the g.c.d of 225 and 30, thus $I + J = (15)$.

(b) $I \cap J$ contains the common multiples of 225 and 30, i.e. is generated by the l.c.m. of 225 and 30, thus $I \cap J = (450)$. 
(b) $I \cap J$ contains the multiples of $225 \cdot 30$, thus $I \cap J = (6750)$.

7. Let $\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}$ be the field with two elements. Find the greatest common divisor $d(x)$ of the polynomials $f(x) = x^5 + x^4 + x$ and $g(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$. Also, find $a(x), b(x) \in \mathbb{Z}_2[x]$ with $d(x) = a(x)f(x) + b(x)g(x)$.

**Solution:** We apply the Euclidean algorithm. Using polynomial division we find:

$$f(x) = (x^3 + x + 1)g(x) + (x + 1)$$

and then:

$$g(x) = (x)(x + 1) + 1$$

Thus:

$$d(x) = \text{g.c.d.}(f(x), g(x)) = 1.$$ 

We also see that:

$$d(x) = g(x) - x(x + 1) = g(x) + x(f(x) - (x^3 + x + 1)g(x)) = xf(x) + (x^4 + x^2 + x + 1)g(x).$$

(Note that in the field with two elements there is no difference between “+” and “−”.)

8. Given a polynomial $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ in the polynomial ring over a field $K$ and an element $c \in K$, let $p(c) = a_0 + a_1 c + \cdots + a_n c^n \in K$ be the evaluation of $p(x)$ at $c$. Show that $p(c)$ is the remainder of the division of $p(x)$ by $x - c$.

**Solution:** By the Division algorithm for polynomials there exist polynomials $q(x)$ and $r(x)$ in $K[x]$ such that $p(x) = q(x)(x - c) + r(x)$ and $\deg r(x) < \deg (x - a)$ or $r(x) = 0$. This means $r(x)$ is a constant $s \in K$, i.e. one has $p(x) = q(x)(x-c)+s$. Evaluating this equation at $c$ gives $p(c) = q(c)(c-c)+s = q(c)0+s = s$ as required. Note that we have used here that the evaluation of a product or sum is the product or sum of the evaluated factors resp. summands, i.e. evaluation at $c$ is a ring homomorphism from $K[x]$ to $K$. This follows immediately from the definition of the ring structure of $K[x]$. 